Content Management and Protection in Smart Cities IP – Based Backbone Wireless Sensors Networks

A. Fragopoulos, J. Gialelis, D. Serpanos
Presented by: A. Papalambrou

Work supported by:
• CHIRON Project JU ARTEMIS Grant Agreement # 2009-1-100228 and
• nSHIELD JU ARTEMIS Grant Agreement # 2010-1-269317
Paper Outline

• Introduction - Objectives
• IP based Backbone Networks in the context of smart environments
• MPEG-21 Standard Related Parts
• Proposed Architecture
• Implementation Issues
• Conclusions – Future Work
Introduction

• IP based Backbone Networks in the context of smart environments,
• Smart environments create sensitive “content”,
• New emerging frameworks for secure digital contents delivery and consumption are required,
• Lack of a generic approach for DRM in such environments,
• Utilization of new emerging standards like MPEG-21, may be very helpful.
Objectives

• Secure networking with DRM support (IP protection)
• Seamless integration of various security technologies (trusted platforms, network security technologies, tamper-resistant devices, etc.)
• Simplicity, efficiency and low cost
• Scalability, Interoperability
• Architecture with security & DRM functionalities incorporating:
  – MPEG-21 Rights Expression Language (REL)
  – Intellectual Property Management and Protection (IPMP)
  – Trusted DRM client
• Prototype of integrated secure network multimedia service with DRM over interconnected IP based backbone WSNs
IP based Backbone Networks in the context of smart environments

User-Converged WWBAN in the framework of Smart Environments
MPEG-21 Related Parts

• New standard in the multimedia world, that allows the seamless and interoperable delivery of multimedia digital contents to the end-users in a dynamic environment.

• Related Parts of the Standard
  – **MPEG-REL**, defines the Rights Expressions semantics for the generation of usage licenses,
  – **MPEG-21 IPMP**, provides semantics and mechanisms for incorporating security tools for protection of digital item, acting as the MPEG’s term for DRM.
MPEG-21 REL Model

```
<r:license>
  <r:grant>
    <r:keyHolder>
      <r:info>
        <dsig: keyValue>
          <dsig:RSAkeyValue>
            .........
          </dsig:RSAkeyValue>
        </dsig: keyValue>
      </r:info>
    </r:keyHolder>
    <mx:play/>
    <mx:diReference>
      <mx:identifier>urn:music:example:001</mx:identifier>
    </mx:diReference>
    <r:allConditions>
      <r:validityInterval>
        <r:notBefore>2008-05-01T00:00:00</r:notBefore>
        <r:notAfter>2008-05-31T00:00:00</r:notAfter>
      </r:validityInterval>
      <sx:ExerciseLimit>
        <sx:Count>10</sx:Count>
      </sx:ExerciseLimit>
    </r:allConditions>
  </r:grant>
</r:license>
```
MPEG-21 IPMP

MPEG-21 IPMP in conjunction with the MPEG-REL provide a framework that enables content “creators” to pertain their rights and interests in digital items and to have the assurance that those rights and interests will be persistently and reliably managed and protected.
High Level Architectural View

DRM Process Model

- Content Owner
  - Creates Digital Content
- License Provider
  - License Creation
  - Creation of Packaged License (embed CEK to License)
- User
  - Process Packaged Content
  - Content Renderer
Implementation Issues (2)

Schematic View of MPEG-21 License Generation

Encrypted Packaged License
Implementation Issues (3)

DRM CLIENT APPLICATION

Generic Architectural View

Core Modules

ISSPIT 2013, 12-15, December 2013, Athens, Greece
Conclusions – Future Work

• Interoperable DRM architecture that apply in IP based Backbone Networks in the context of smart environments, which utilizes the semantics of MPEG-21.

Future Work

• Enhancement of the applications’ server embedded DRM architecture, in terms of processing, storage and energy consumption.

• Utilization of MPEG-21 IPMP in the same context

• Further usage of security mechanisms, e.g. Trusted Platforms, Tamper-proof components, etc.

• Appliance of same approach to other areas, e.g. e-health security framework
THANK YOU,
FOR THE ATTENTION