

Towards an extensible core model for Digital Rights Management in VDM

Rasmus Lauritsen
Ph.D. Student
Department of Engineering
Aarhus University

rala@iha.dk

Lasse Lorenzen
System Architect
Audio R&D
Bang & Olufsen

llz@bang-olufsen.dk

10th International Workshop Overture

C O M P A S S

www.compass-research.eu



Introduction to this work

VDM models created

Comparison

Towards an extensible core model for DRM

Conclusion

Introduction to this work

VDM models created

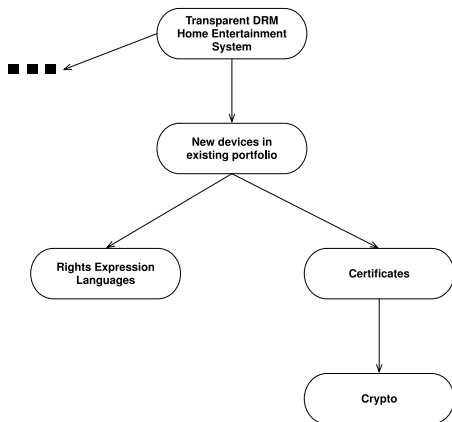
Comparison

Towards an extensible core model for DRM

Conclusion

Motivation

Whether and to which extent can modelling assist in making DRM transparent in a HES?



Approach

Goal: One extensible core model

- ▶ Two different views on DRM were modelled in VDM
 - ▶ A User-Centric view
 - ▶ A Business-Centric view
- ▶ Each view is treated as a candidate core model
- ▶ One Case property for DRM modelled using each core model
- ▶ Common traits has been derived from the VDM models
- ▶ A sketch for a core model has been derived

The two DRM properties considered

The two DRM properties considered

Case Question

Whether and to which extent is it feasible to model DRM integration before consumer device entry to an existing portfolio?

The two DRM properties considered

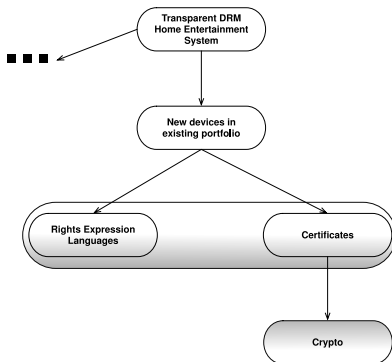
Case Question

Whether and to which extent is it feasible to model DRM integration before consumer device entry to an existing portfolio?

Case Question

Whether and to which extent can cryptographic and security properties be modelled?

The two DRM properties considered



Introduction to this work

VDM models created

Comparison

Towards an extensible core model for DRM

Conclusion

VDM models created

- ▶ **User-Centric core model** - Based on Popescu et al. focusing on the device configuration at the users site.

VDM models created

- ▶ **User-Centric core model** - Based on Popescu et al. focusing on the device configuration at the users site.
- ▶ **Extended User-centric model** - Extending the user centric model.

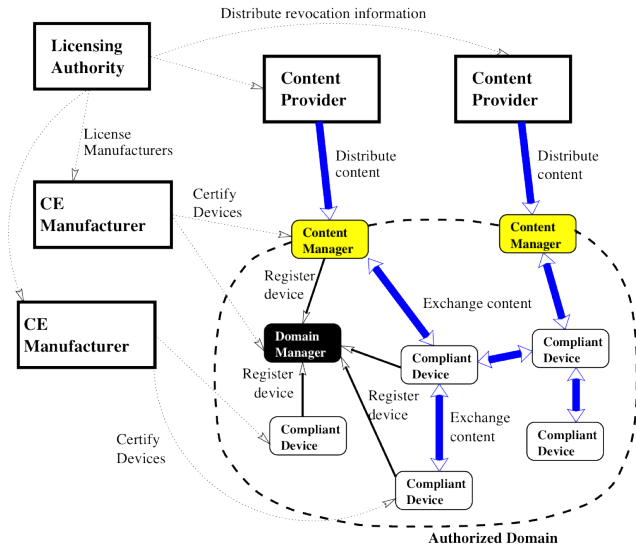
VDM models created

- ▶ **User-Centric core model** - Based on Popescu et al. focusing on the device configuration at the users site.
- ▶ **Extended User-centric model** - Extending the user centric model.
- ▶ **Business-Centric core model** - Based on Ku et al. focusing on business aspects and aims at being complete.

VDM models created

- ▶ **User-Centric core model** - Based on Popescu et al. focusing on the device configuration at the users site.
- ▶ **Extended User-centric model** - Extending the user centric model.
- ▶ **Business-Centric core model** - Based on Ku et al. focusing on business aspects and aims at being complete.
- ▶ **Crypto Parameter Consistency** - Extending the business centric model.

User-centric DRM view



VDM model of the User-centric DRM view

Results

- ▶ Product introduction
- ▶ Combinatorial testing
- ▶ Control Point added
- ▶ Off and On-line testing

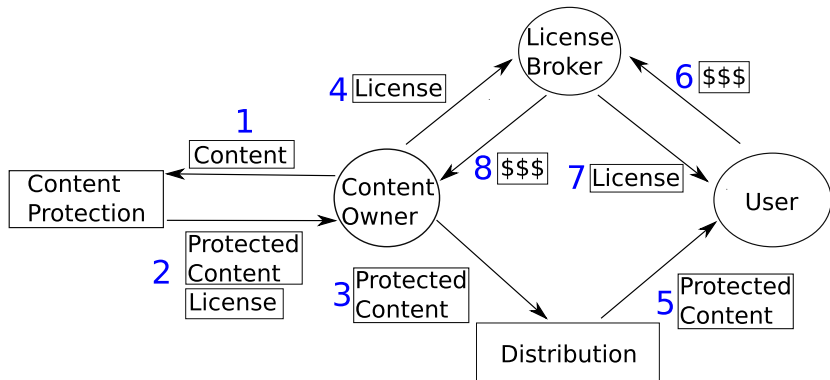
The core model

- ▶ CEDevice
- ▶ CEManufacturer
- ▶ Certificate
- ▶ ContentManager
- ▶ ContentProvider
- ▶ DomainManager
- ▶ LicensingAuth
- ▶ Content

Extensions for the core model

- ▶ ControlPoint

Business-centric DRM view



VDM model of the Business-centric DRM view

Results

- ▶ Link between content protection and viewer
- ▶ Extensibility through inheritance
- ▶ Easy to extend
- ▶ Crypto externalised

The core model

- ▶ Content
- ▶ ContentOwner
- ▶ ContentProtection
- ▶ Distribution
- ▶ License
- ▶ LicenseBroker
- ▶ ProtectedContent
- ▶ Viewer
- ▶ ProtectionDomain

Extensions for the core model

- ▶ CryptoParameters
- ▶ CryptoProtectionDomain

Introduction to this work

VDM models created

Comparison

Towards an extensible core model for DRM

Conclusion

Comparison

Entity	User-centric DRM view	Business DRM view
Content Provider	Yes	Yes (Distribution)
Licensing Auth	Yes	No
CEManufacturer	Yes	No
Content Manager	Yes	No
Domain Manager	Yes	No
Compliant Device	Yes	Yes (Viewer)
Viewer	Yes (Compliant Device)	Yes
License Broker	Yes (Content Provider)	Yes
Distribution	Yes (Content Provider)	Yes
Content Owner	No	Yes
Content Protection	No	Yes
Content	No	Yes
Protected	No	Yes
License	No	Yes
Money	No	Yes
Protected Domain	Yes (Auth Domain)	No

Comparison

Entity	User-centric DRM view	Business DRM view
Content Provider	Yes	Yes (Distribution)
Licensing Auth	Yes	No
CEManufacturer	Yes	No
Content Manager	Yes	No
Domain Manager	Yes	No
Compliant Device	Yes	Yes (Viewer)
Viewer	Yes (Compliant Device)	Yes
License Broker	Yes (Content Provider)	Yes
Distribution	Yes (Content Provider)	Yes
Content Owner	No	Yes
Content Protection	No	Yes
Content	No	Yes
Protected	No	Yes
License	No	Yes
Money	No	Yes
Protected Domain	Yes (Auth Domain)	No

Comparison

Entity	User-centric DRM view	Business DRM view
Content Provider	Yes	Yes (Distribution)
Licensing Auth	Yes	No
CEManufacturer	Yes	No
Content Manager	Yes	No
Domain Manager	Yes	No
Compliant Device	Yes	Yes (Viewer)
Viewer	Yes (Compliant Device)	Yes
License Broker	Yes (Content Provider)	Yes
Distribution	Yes (Content Provider)	Yes
Content Owner	No	Yes
Content Protection	No	Yes
Content	No	Yes
Protected	No	Yes
License	No	Yes
Money	No	Yes
Protection Domain	Yes (Manufacturer)	No

Introduction to this work

VDM models created

Comparison

Towards an extensible core model for DRM

Conclusion

Towards an extensible core model for DRM

Findings Summary

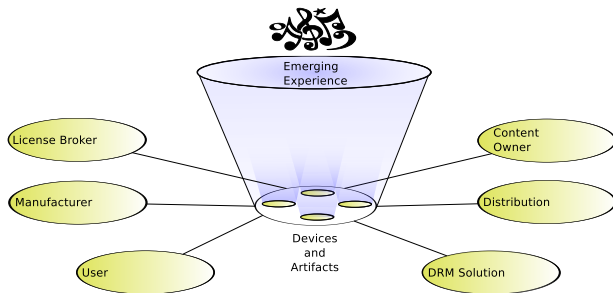
- ▶ The business centric core model has a simplified user setup. The User-centric core model has a richer user setup including device and manufacturer.
- ▶ The business centric core model does not capture distribution of license access resulting in more complicated model setup harness.
- ▶ Content Provider in the User-centric core model is split between License Broker and Distribution from the business centric core model
- ▶ Content Protection is explicit in the business-centric core model but implicit in the user-centric core model.

Towards an extensible core model for DRM

With the above findings we approach the challenge of Developing a suitable abstraction by having:

- ▶ Entities: Content Owner, Distribution, User, Manufacturer, License Broker, DRM Solution (Content Protection), Device and Artifacts.
- ▶ Need for consistent framework/terminology.
- ▶ Keeping the goal of allowing the Manufacturer to achieve Conform-ability with the chosen DRM solution in mind.
- ▶ The core model approach: one model and terminology to capture a variety of DRM properties.

Towards an extensible core model for DRM



Unified concepts derived from the two core models put graphically.

Introduction to this work

VDM models created

Comparison

Towards an extensible core model for DRM

Conclusion

Conclusion

- ▶ The core model approach seems to pay off
- ▶ We have a preliminary estimate for a core model for DRM in VDM
- ▶ The two case properties were successful:
 - ▶ We can find all illegal combinations before we try to introduce the device to the portfolio
 - ▶ We can model cryptographic and security properties

Future work

- ▶ Try the core model on a real DRM systems like:
 - ▶ Google Widewine DRM solution
 - ▶ Microsoft PlayReady DRM solution
- ▶ More iterations with example case properties
- ▶ Revise and refine the core model as needed
- ▶ Our model is not complex enough to catch boundary cases such as:
 - ▶ Spotify - no playback on wireless speakers
 - ▶ Pink Floyd - only to be played as albums

Introduction to this work

- Motivation

- Approach

- Two DRM case properties

VDM models created

- User-centric DRM view

- Business-centric DRM view

Comparison

Towards an extensible core model for DRM

- Findings Summery

- Derived core model put graphically

Conclusion

- Future work

Questions?