European Technology Platform *NEM*
Networked and Electronic Media

Trust, Security & Dependability (TSD) Challenges & Issues

James Clarke

Waterford Institute of Technology

NEM Big Challenges[1]

- To create interoperable network infrastructures to enable seamless multimedia networking
  - universal access to and creation of digital electronic media & content delivered over a full range of networks and channels.
- To empower end users by putting the user first
- To promote "electronic content from all to all"
  - all aspects of work, personal/private life, and leisure, accessible any time, any place, and presented in *right* context
- To merge the various media and content formats
- To develop new middleware for media applications.

[1]**Source:http://www.nem-initiative.org/Documents/NEM-BC-001.pdf**

TSD in NEM – overview
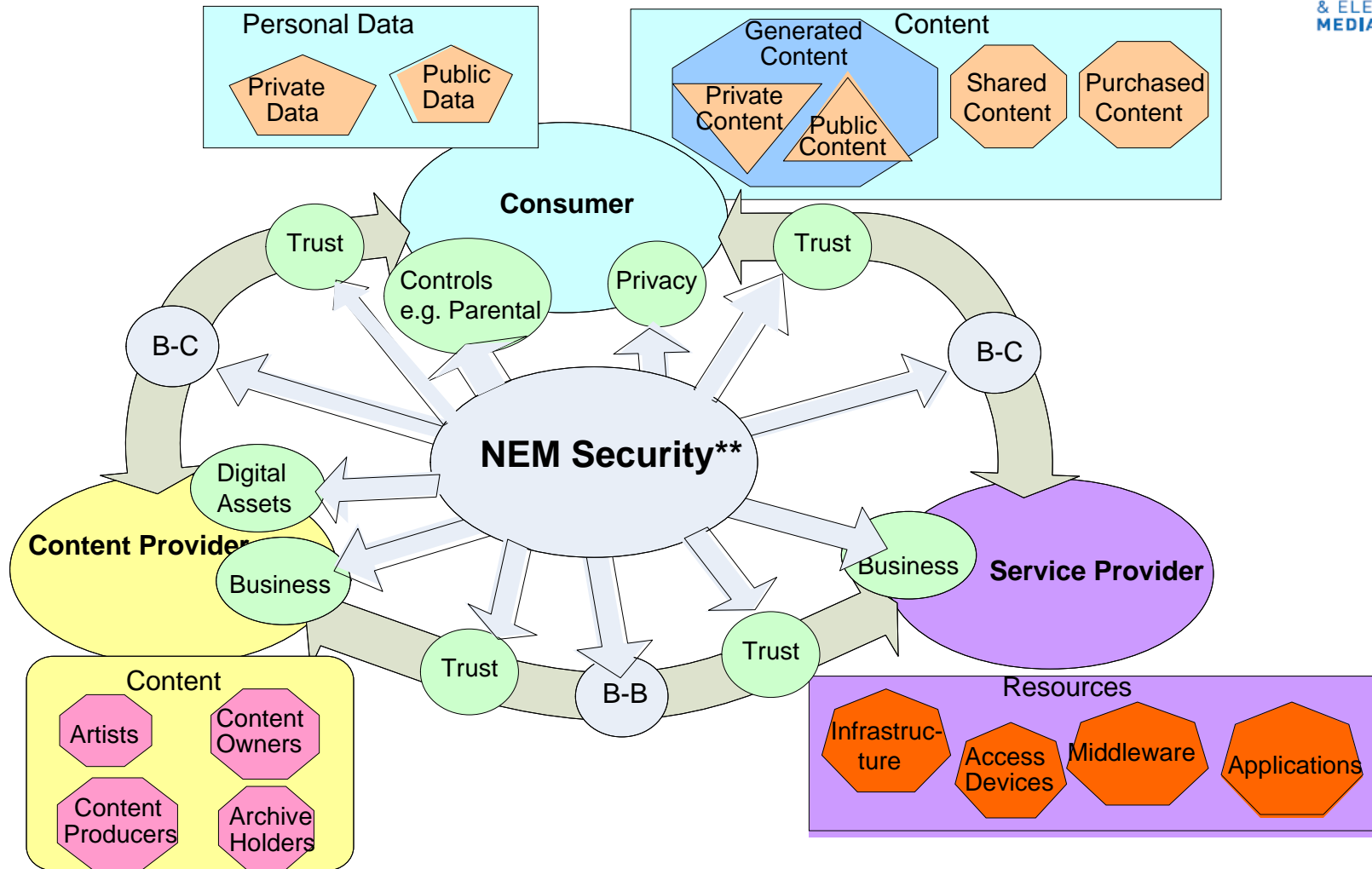
NEM Security contains legal/regulatory issues, security technologies, contract creation & management, rights management, identity management, trust aspects, authentication and intrusion detection and isolation, ….

NEM stakeholders

- Consumer/user
  - users, clients: private individuals, workers, enterprises, organisations;
  - Set-top box owners (satellite, cable and/or IP device in the future) ;
- Content provision
  - Traditional broadcast stations who make their own content
  - Third party content produces who supply stations
  - Other forms of content providers
    - evolving multimedia and information providers
    - information archives and data-vaults
    - ……………
- Service provision
  - system equipment and product suppliers
  - service and application software suppliers
  - service creators and deliverers
  - interconnect/communication operators (broadcast, cable, satellite, IP,..)
- Strategy and oversight
  - technical strategists, researchers, and developers;
  - R&D community: academic, commercial, and industrial sectors;
  - industry regulators (e.g. ITU WG on Identity Management)
  - Member State interests;

TSD in NEM – Current SRA V5.0[2]

- Security – yes – essential, but also need
  - Trust: need to *trust* content, source/origin and context
  - Dependability: must be available and work as offered/accepted.

- **Security** and **privacy**
  - requirements concerning privacy, integrity, accountability, and the mechanisms to support them
    - identification, authentication, authorization, (non)-repudiation;
    - Analysis of implications of the integration of business models from the media and telecoms industry e.g. personalised targetted advertising.

[2]**Source:http://www.nem-initiative.org/Documents/NEM-SRA-050.pdf**

TSD in NEM – Current SRA V5.0

- **Identity Management**
  - A token for gaining access to media services and terminals.
  - Three lines of research identified:
    - Physical methods of ID (HW, SW, combinations)
    - Ensuring interoperability amongst services and appls.
    - Ensuring an appropriate level of privacy.

- **Regulatory aspects**
  - Market for NEM is a global one, yet no enforceable global regulation.
  - Limits free movement of NEM and presents security challenges (SPAM, DoS, …)

TSD in NEM – Current SRA V5.0

- Trust in the Digital rights management technologies

  - For whole value chain: content originators - consumers
  - Guarantee trusted environment between terminal and rights mgmt platform
  - Verification that content is not tampered with or damaged in delivery

Next Version of SRA.
Additional TSD Dimensions

- instilling **trust** in the systems and keeping in a **dependable** condition. Areas of future r&d:
  - the definition of trust: total, partial and assigned trust;
  - protocols for establishing trust;
  - the range of trust models (based on reputation, frequentation or surveillance, on security or redundancy mechanisms) with regard to system, a service, a network, a hardware or software component, or an architecture;
  - the variables to measure trust in real time in a system;
  - the assessment of trust by a user, an operator, a content/service provider, …
- security issues related to **Human and Social aspects.**
  - What are, what will be and what should be the social implications of the development, deployment and use of such NEM systems.
  - Necessary controls built-in. e.g. Parental controls.

Next Version of SRA.
Additional TSD Dimensions

- **Empowerment** of the User:
  - Paradigm shift giving more control to the users;
  - Stronger user-centric identity management and deployment (Identity layer);
  - Improve control on privacy and identity related aspects from the perspective of citizen;
  - Whilst operating across distributed and multi-operators platforms.
  - Purpose based access control: In addition to techniques protecting personal information before disclosure, new approaches to protect information after disclosure.

Next Version of SRA.
Additional TSD Dimensions

- security for **user generated content**:
  - lots of filtering to find a small amount of interesting material from within a large amount of potentially uninteresting material;
  - Currently, the most interesting available content is controlled by user subscription to content providers (music, podcasts, photos, video, …) on relevant content to ones self and whose authoring processes are high enough quality;
  - real value of user generated content is within a more strictly controlled environment with trustworthy, secure and dependable distribution mechanisms.

- Security of **Digital Assets Management**
  - much wider implications than information management in general: it includes management of Intellectual Property Rights (IPR), Digital Rights Management (DRM), copyrights and online sharing of information.
  - The security objectives related to the digital assets are
    - confidentiality (non-disclosure to unauthorized persons),
    - integrity (non-alteration of content by hackers), and
    - availability (the availability of licensed users to use these assets without being hindered by unintentional or malicious acts.

Next Version of SRA.
Additional TSD Dimensions

- **security** and **scalability**:
  - different manifestations individually and combined;
  - Security needs to be cross-considered with Scalability facets: with respect to sizing, performance, capacity planning, stability, etc.)
  - Adaptive security for scalabilty purposes e.g. resource constrained situations
  - Examples of system/application areas:
    - Pervasive computing
    - Peer-to-peer
    - Distributed and collaborative computing
    - Mobile communications

NEM Security Working Group – *what next?*

- NEM Security WG to complete wish list for next iteration of SRA
  - NEM SEC. Position paper in progress;
- NEM SEC WG to examine new TSD project portfolios.
- NEM SEC WG to examine cross-overs between other eTPs to see if there are synergies (this event will greatly assist)
- If interested to participate, please contact me at **<jclarke@tssg.org>**