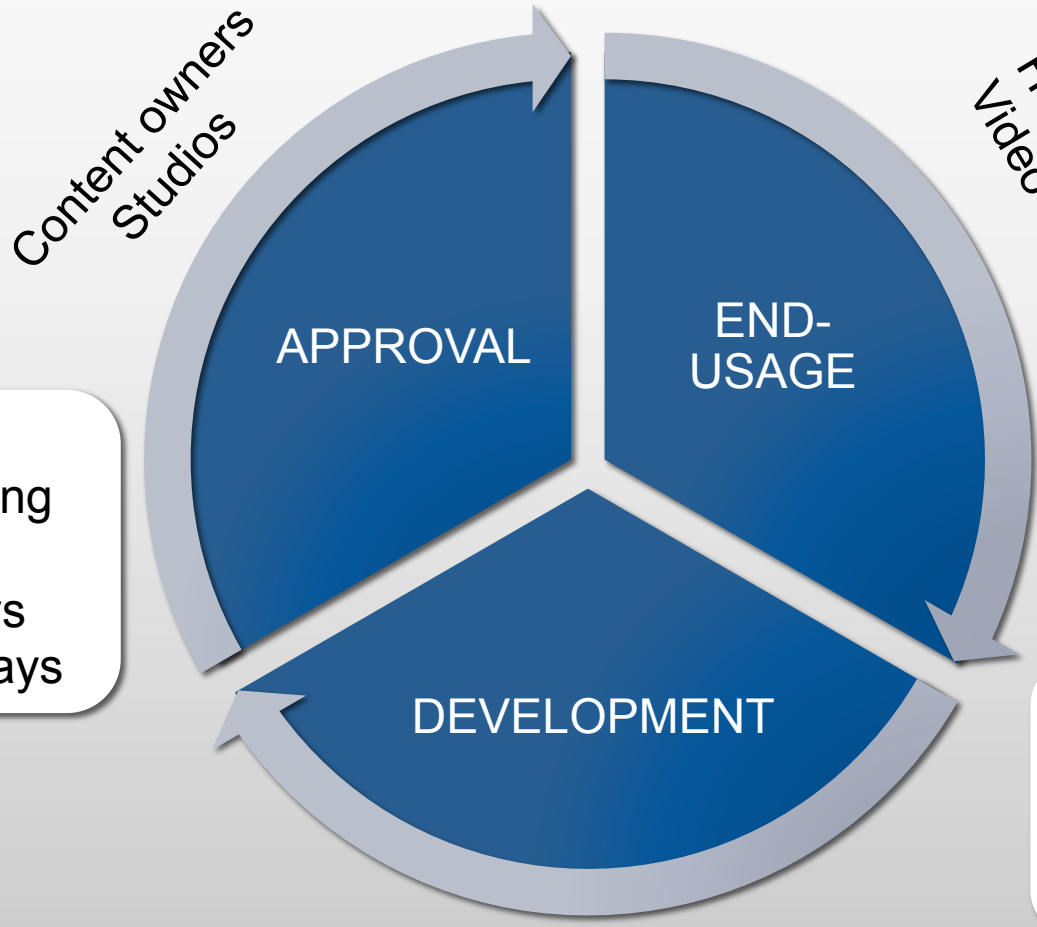
SECURITY EVALUATION AND CERTIFICATION FOR PREMIUM CONTENT

Carolina Lavatelli, Internet of Trust

HPA Tech Retreat - Indian Wells, Feb 11th 2015

THE CHALLENGE OF THE SECURITY SCHEME



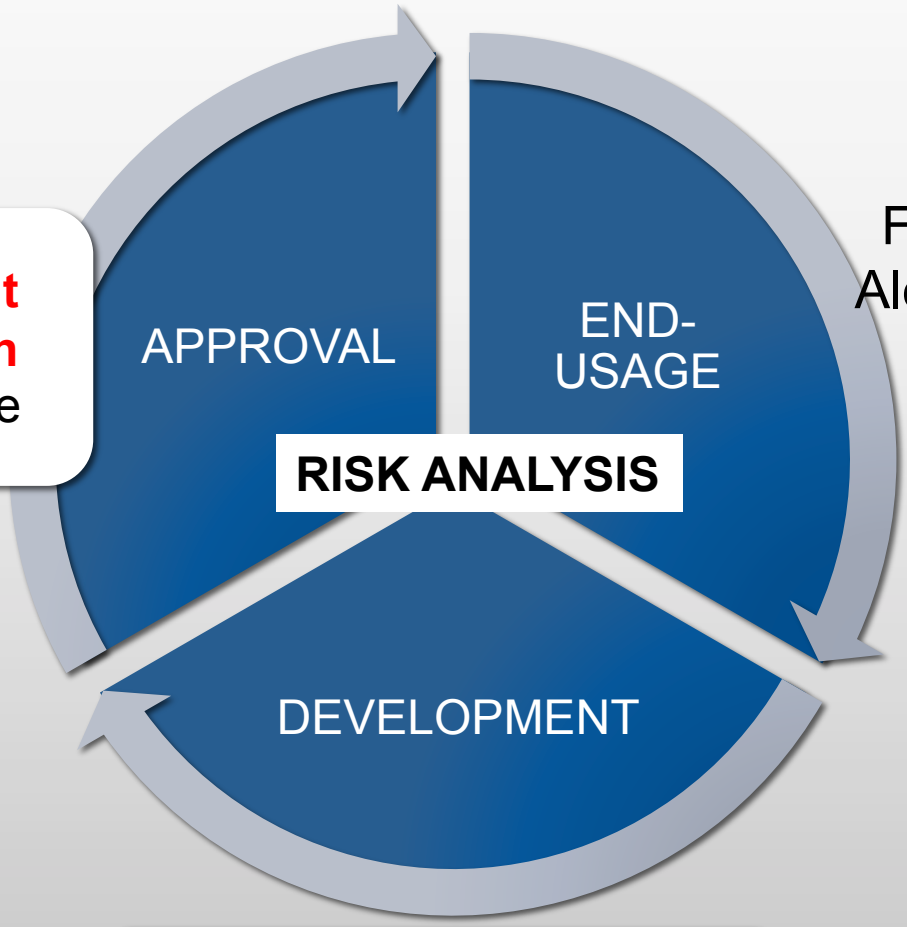
CHALLENGE
Size the underlying « security requirements » vs risk & cost & delays

INDUSTRY CONSTRAINTS
Mass-production
Time-to-market

TV / tablets / smartphones industries
Technology providers, chipset manufacturers, SW providers, Integrators

SECURITY IS MULTI-FORM

Security Assessment
Security Certification
Functional Compliance



Contracts
Field Monitoring
Alert Management

Security-by-Design
Standardized Dev. Process
Organisational Measures

SECURITY-BY-DESIGN

- SOFTWARE
  - Sound protocols and cryptography
  - Sound data access and flow control policies
- HARDWARE
  - Technology maturity
  - Well-defined measurement techniques
- ARCHITECTURE
  - Minimum set of functions and components
- TOOLS & METHODS
  - modeling, proofs, static analysis, automatic test generation, etc.

ROOT-OF-TRUST
TRUSTED EXECUTION ENVIRONMENT (TEE)

SECURITY ASSESSMENT

- BACKGROUND
  - Consolidated risk analysis

- EVALUATION REFERENTIAL
  - Minimum set of technical requirements for the product
  - Harmonized evaluation techniques

INDEPENDENT ASSESSMENT

- Test performed by independent skilled and equipped lab (ISO17025)
- The lab performs independent vulnerability search

SELF-ASSESSMENT

- Internal teams may lack time, knowledge or means to reach state-of-the art testing techniques
- Conflict of interest

CERTIFICATION & APPROVAL

- CERTIFICATION role
  - Laboratory licensing (audits)
  - Harmonized evaluation methodology across labs
  - Definition and maintenance of « security requirements »
  - Evaluation monitoring

- APPROVAL
  - Commercial authorization
  - Security is one of the key aspects, not the only

- The approval entity can play the certification role

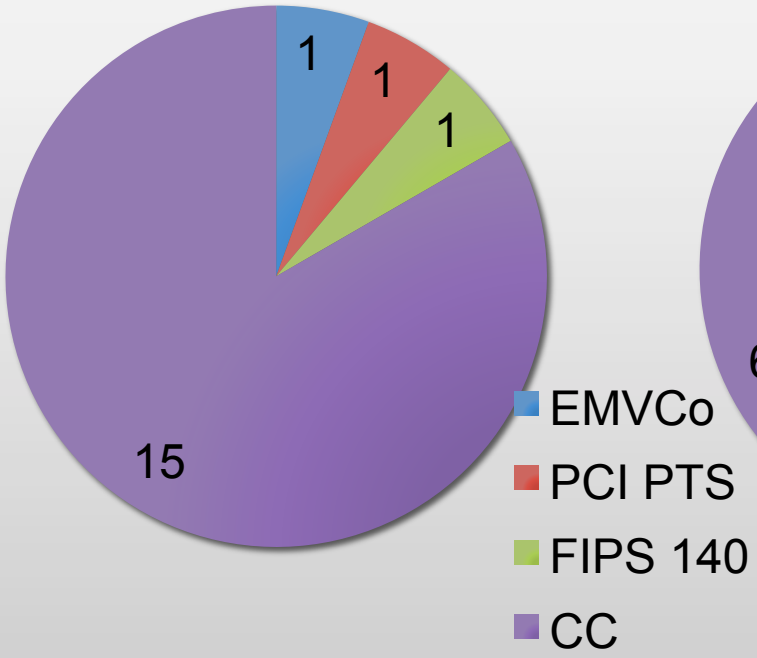
SUMMARY

- EVALUATION REFERENTIAL
  - Common understanding
  - Transparency
- INDEPENDENT ASSESSMENT
  - Confidence (absence of conflict of interest)
  - State-of-the-art testing
- INDEPENDENT CERTIFICATION
  - Neutral layer between the lab and the approval entity
  - Harmonization across labs

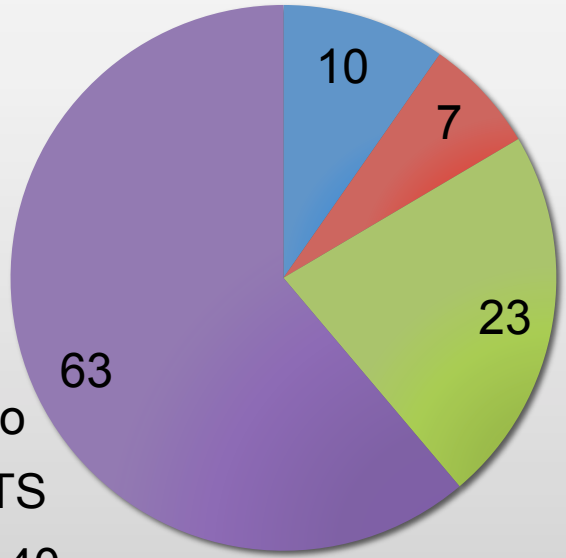
HOW OTHER SCHEMES BEHAVE

(focus on payment, crypto and all IT systems)

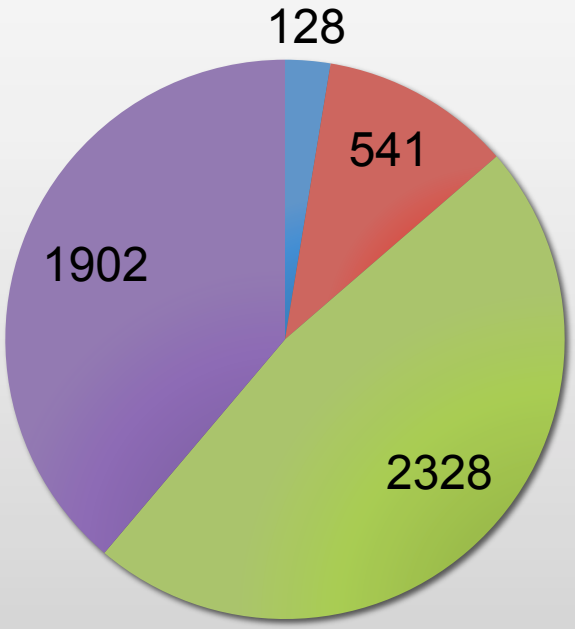
Certification entities



Labs



Certificates



Sources
www.emvco.com
www.pcisecuritystandards.org
www.csrc.nist.gov
www.commoncriteriaportal.org

EMVCo: valid certificates
PCI PTS: valid certificates
FIPS: all 1995-2015 (235 in 2014)
CC: all not archived (817 IC & smartcard)

THANK YOU

carolina.lavatelli@internetoftrust.com