



⇒ The secure, open standard for digital content protection

# Secure Video Processor

## *Open Platform for Content Protection*

Eli Hibshoosh  
Ehibshoosh@ndsisrael.com



→ The secure, open standard for digital content protection

SVP Members



SVP Associates



## □ Set the driving principles for

- - **E2E Security**
  - **Open Content Protection model**
  - **Interoperability** for consumers and devices

- ❑ **Enable the interests** of all the players: from content creators, distributors...device manufacturers, **consumers**
  - E.g., robust security, level-field competition, cost, interoperability
- ❑ **Pay TV security** lessons applied cost-effectively to “horizontal” market to promote hi-quality content consumption
- ❑ **Enable interaction** between the CA/DRM and standard SVP Open-CP
- ❑ **Flexibility** Built-in to allow the market to reach its equilibrium – **Enabling not Mandating rules, e.g.,**
  - **No immutable encoding rules;**
  - **Embracing technological change**

## Threats:

- ❑ Theft and distribution of clear content
- ❑ Theft and distribution of broadcast (global) keys - McCormac
- ❑ Circumvention of content usage rights
- ❑ Technology potentially outpaces protection
  - BB, Internet, p2p, compression tools, SW debug tools, ubiquitous cheap storage, media writers...
  - Broadcast-key servers to non compliant devices
- ❑ Regulation – questionable role and sluggish relative to technology

## Opportunities:

- ❑ Quality content, secure, profitable, ... **Anytime, Everywhere**



# SVP Open Content Protection (CP) - Inside the Device

⇒ The secure, open standard for digital content protection

## CA/DRM Business Model Enforcement

Usage Model Definition and Billing

CA / DRM / FTA Agent

## Open CP

TRS-SW Enforcement for (Domain, Proximity, B-Flag, Private Extensions)

SW Chip Driver

Secure Boot Loader in HW

**Core Security Functions:** Certificates handling, SAC, CryptoTools., Time, Key-Mgmt, Content License (UsageRules & content-keys), Export content control, revocation

**Content processing:** Content De/Scrambling, Content Decoding

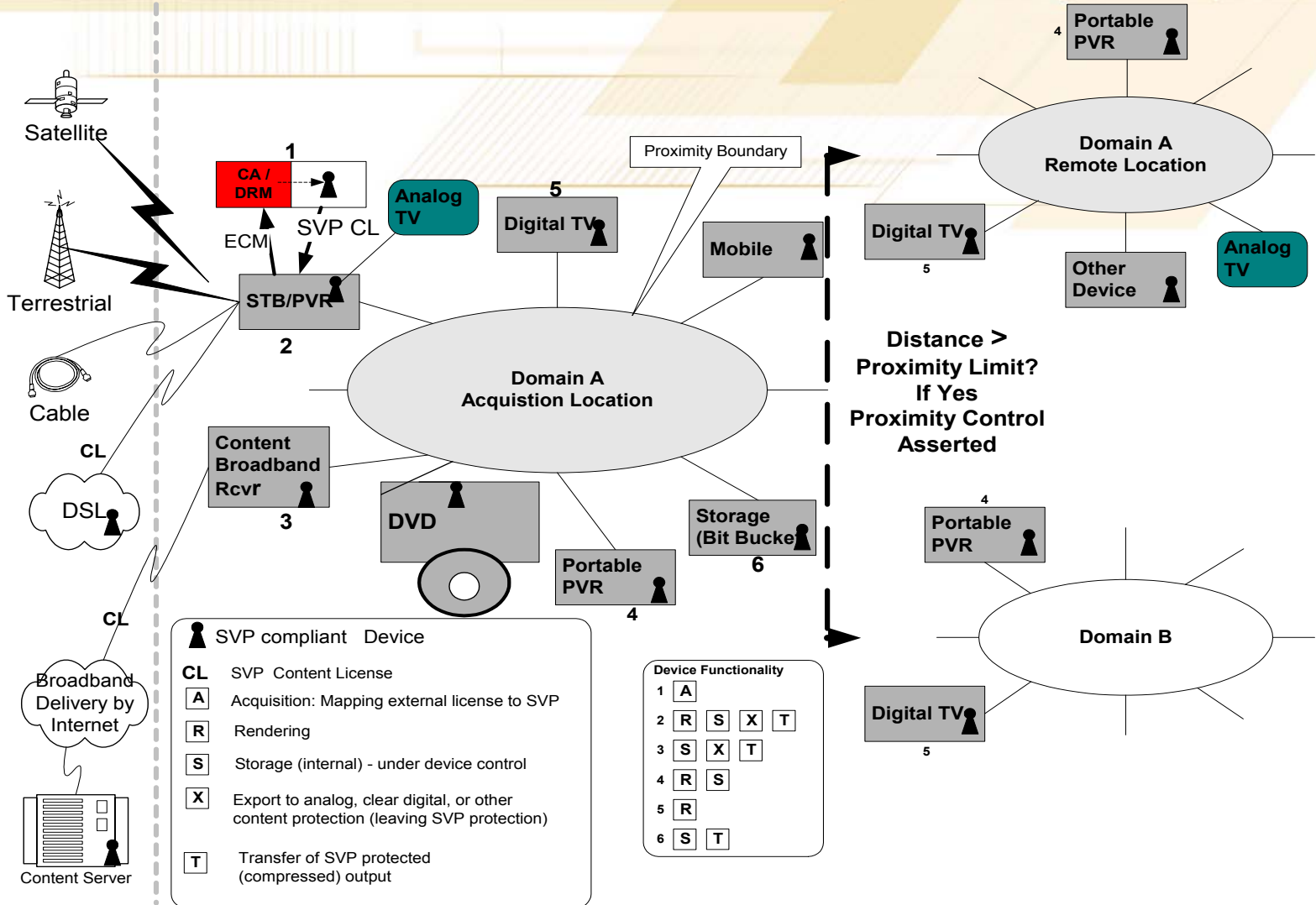
**HW Chip Requirements e.g, Personalization, Compliance and Robustness**

SOFTWARE

HARDWARE

# SVP – Home Network and Beyond

⇒ The secure, open standard for digital content protection



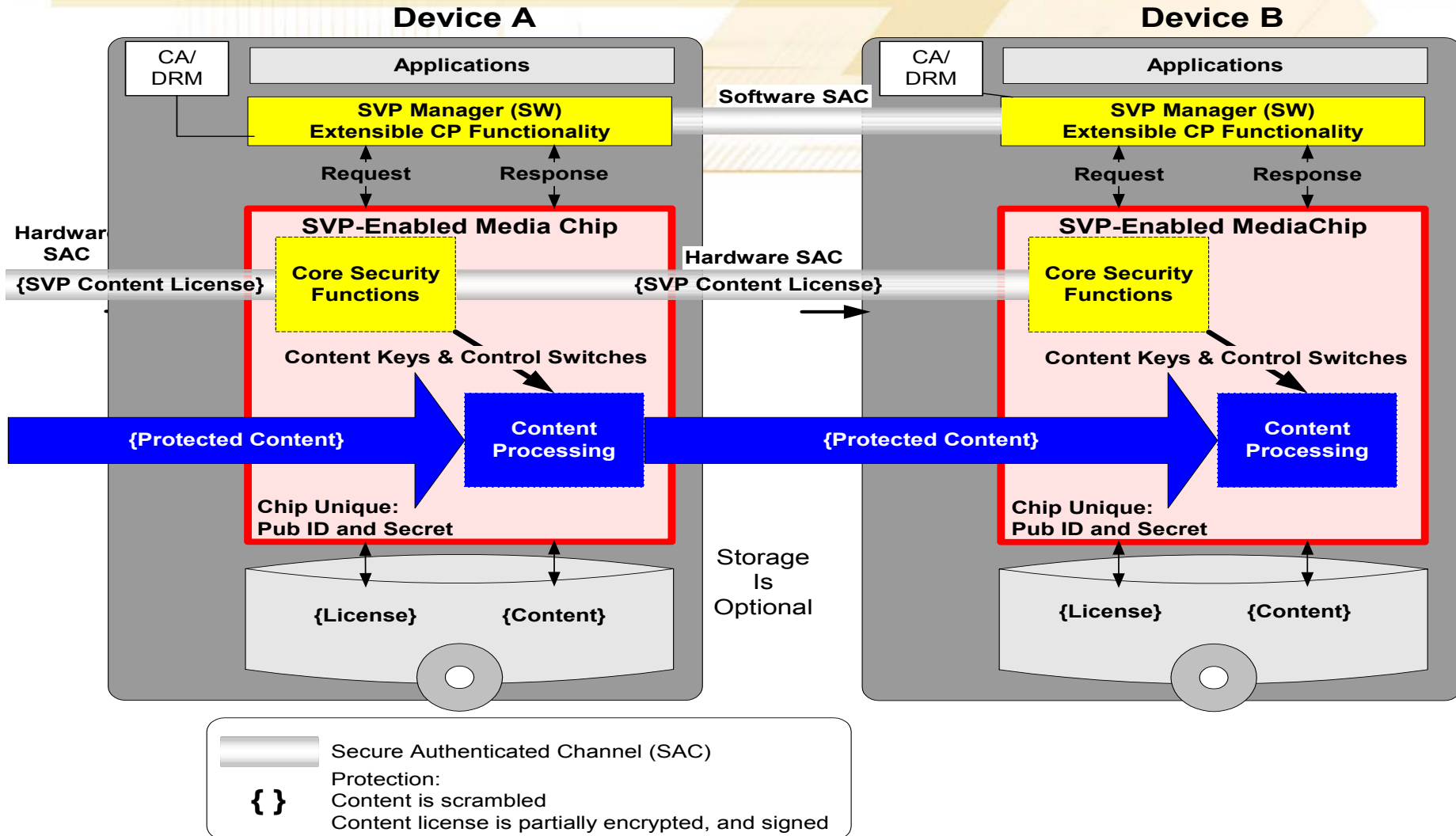
# Open Content Protection (CP) Operational Definition

⇒ The secure, open standard for digital content protection

- ❑ **Enforce Spatial and Temporal content-usage rights related to**
  - Acquisition
  - Consumption
  - Storage (Copy/Move)
  - Distribution: intra- (Proximity) and inter-user domain
  - Content processing, e.g., watermarking detection/insertion
  - Time (Retention, rental control)
  - Export to other approved CP systems
  - Analog-hole - Map analog protection
  - “Adoption” by network operator
  
- ❑ **Shared content control - Enable **Persistent** CA/DRM control: Interaction between: Open-CP (standard SVP in horizontal device) with CA/DRM systems**

# Inter-Device

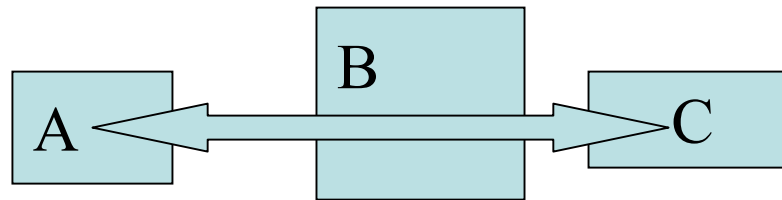
⇒ The secure, open standard for digital content protection



# SVP E2E Security for Compressed Content

⇒ The secure, open standard for digital content protection

- ❑ Under SVP E2E: Clear Content and its License (content keys & rights) are always inside secure chip silicon, Not in the device!
- ❑ No global secrets in SVP; Only single device compromise is possible; no system-wide compromise
- ❑ Recovery of a single device compromise via revocation
- ❑ Content encrypted by Unique-Device-Key or Domain-Key
- ❑ When content goes from device A to C through B, unlike pipe protection, only A and C know the encryption keys



# Interoperability

## ❑ Via Compliant Acquisition

- Input from any CA/DRM
- Input from Fixed-media Many-to-One content protection system
- Input from VOD server

## ❑ Controlled Export to Authorized CP systems

- Desirable - To enhance security export-CP is built into SVP chip
- Less desirable - clear content is exported to Authorized CP in the device; protected by device compliance & robustness rules

- Certificates Tree**
- Certification authority: Root or manufacturer or network operator**
- Device Attributes, restrictions on content usage**
- Certificate attributes and content license**  
**Together determine content usage ( in conflict – use the stricter of the two)**
- Issuer: Device manufacturer, Network operator**

- Content revocation – content license specifies whether the content is to be sent to (accessed) by a revoked device**
- Revocation criteria/procedure**
- CRL – list of revoked device IDs delivered securely via SAC**



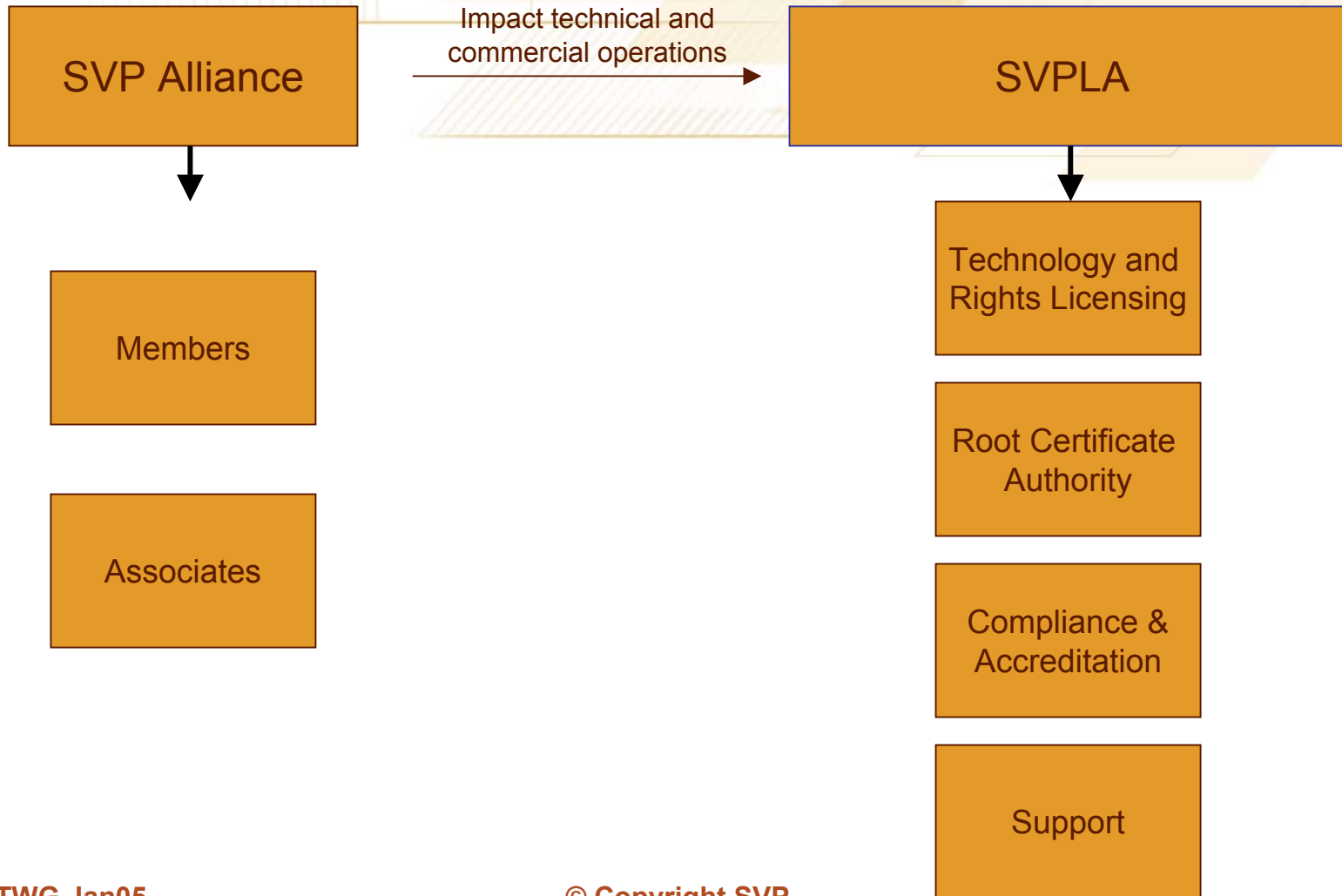
# Compliance and Robustness (C&R) the What and How

⇒ The secure, open standard for digital content protection

- ❑ Acquisition point and SVP-enabled Media Chip must be externally certified by accredited SVPLA lab.
- ❑ Media devices are certified either by:
  - External entity - By accredited SVPLA lab, or
  - Internal entity - By device manufacturer
- ❑ Acquisition points (examples):
  - Smart Card
  - Fixed Media
  - VOD server at the headend

# Organization and Legal

⇒ The secure, open standard for digital content protection



- Publish complete SVP specification
- Set criteria for eligibility for licensing (RaND) and then license
- Operate root certificate authority
- Implement SVP specification change procedures
- Implement revocation procedures
- Establish and implement prices for licensing
- Set rules for compliance and robustness
- Accredit testing labs
- Authorize non-SVP content protection systems as trusted for purposes of Export
- Provide support services

**\*Wholly-owned subsidiary of NDS**

- Act as an advisory committee to SVPLA**
  - Propose changes to specification and procedures
  - Set accreditation rules for testing labs
  - Promote SVP adoption and usage
  - Technical Working Groups
- Initiate and second revocation**
- Lobby standards bodies**
- Responsible for marketing – website, shows and events**
- Encourage interoperability**
  - Recommend non-SVP content protection systems to be authorized as trusted for purposes of export

**\*Not-for-profit organization**



# SVP Advantages - Conclusion

⇒ The secure, open standard for digital content protection

- Open**
- Secure**
- Flexible**
- Low-Cost**
- Interoperable**



**Bottom line**

⇒ The secure, open standard for digital content protection

**For high-quality, valuable content  
the lesson is:**

**Use SVP Open CP!**



# For More Info

⇒ The secure, open standard for digital content protection

[www.svpalliance.org](http://www.svpalliance.org)