***UltraCAS*™ compliance**

With

MovieLabs

Specification for

Next Generation of Video and

Enhanced Content Protection V. 1.1

MovieLabs Specs Set A New Benchmark for Ultra High Definition Content Security

With the rapid adoption of Ultra High Definition television, MovieLabs has published a set of guidelines issued by and for the major studios that is viewed as a new benchmark for how the movie and broadcast industry will protect its latest and best Ultra HD content.

Secure TV, an innovator in the CAS world has developed UltraCAS™ 4K, a CAS designed to meet and exceed the MovieLabs specifications for Ultra HD content security. Secure TV was founded by Bob Kulakowski one of the two founders of Verimatrix and Bob has brought together a team of highly experienced CAS software developers to produce UltraCAS 4K.

This whitepaper presents the requirements from the MovieLabs "Specification for Enhanced Content Protection" Version 1.1 in blue text followed by text explaining how UltraCAS meets or exceeds the MovieLabs requirements.

UltraCAS was designed using the best of ***e-commerce*** and ***on-line banking*** security protocols and algorithms delivering security similar to the security protecting billions of dollars of on-line and banking transactions annually. The amazing level of security built into UltraCAS is cost-effectively deployed by a fully-redundant and scalable highly secure headend. As a result, UltraCAS provides security beyond what is required for Ultra HDTV, with the lowest total cost of ownership of any CAS providing similar protection.

UltraCAS was built from the ground up using proven security hardened technology and includes a FIPS 140-2 Certified Security Core and silicon protected systems keys. FIPS 140-2 Certification in the US is required for government security and is regulated by **Federal Information Processing Standards** (**FIPS**) publications. FIPS Certification assures that state of the art cryptographic algorithms are used in a secure audited manner.

The full text for the MovieLabs Version 1.1 Specification dated February 2015 is available on the MovieLabs website at the following link:
htttp://www.movielabs.com/ngvideo/MovieLabs%20Specification%20for%20Enhanced%20Content%20Protection%20v1.0.pdf

The exact requirements text from the MovieLabs specification are presented below starting with the "Problems/Threats" section on page 2 of the MovieLabs spec. Details on the UltraCAS solution follow the MovieLabs specification.

MovieLabs spec: ***Problems/Threats***

The goal of enhancing content protection is to mitigate certain piracy problems that are not adequately addressed by current practices and to prevent piracy problems that might occur in situations when there are multiple formats and means of distribution carrying the first high quality targets each exposed to different threats.

SecureTV was founded back in 2010 to mitigate the problems inadequately addressed by the existing CAS vendors that relied on smartcards and out of date security techniques.

MovieLabs spec: ***Availability and Distribution of Ripping Software***

Ripping applications appear from time to time, sometimes working across a sufficient footprint with sufficient reliability to be viable as illegal software products. This is enabled by two ***"hack one, hack all"*** *scenarios. First, breaking protection on one device, e.g. a PC + drive combination, breaks it on a wide class of devices. And second, breaking protection on a new title often requires no additional information or technology than breaking it on a recent, previous title.*

UltraCAS uses proven e-commerce and on-line banking security algorithms combined with the enhanced security features built into the latest STB chips along with security layers that individualize each device **preventing a "hack one, hack all" attack.**

MovieLabs spec: **Release Day Availability of Rips**

Often, pristine, pirated copies of the original compressed video are available as soon as the title is released. This is enabled when ripping a new release requires no additional information or technology than ripping a recent, previous one.

Release Day Availability of Rips is prevented by e-commerce and on-line banking based key exchanges for content keys, secure code boot, run-time hack detection, and secure hardware based content key decryption and active hacker detection prevent one hack from being reused on other titles.

MovieLabs spec: **Pre-Release Day Availability of Rips**

With content released on discs, often pristine, pirated copies are available even before the release. This is enabled by the problems presented above, plus leaks in the physical supply chain.

UltraCAS incorporates a secure and protected headend environment including encrypted content ingest for Video-On-Demand (VOD) titles preventing supply chain attacks of content being distributed before release.

MovieLabs spec: **Output Capture**

Hardware devices and software applications can often capture digital, baseband video imagery. In the case of hardware, this is enabled when the hardware protection or hardware supply chain has been compromised. In the case of software, it is enabled when a secure media pipeline is compromised. While ultimately camcording the screen cannot be prevented, it can be addressed by forensic watermarking.

UltraCAS incorporates secure media pipeline hardware drivers enabling the secure media decoder pipeline and enabling the appropriate HDCP content protection level specified by the Studio or broadcaster. In addition, the secure boot, active Hacker detection, run time integrity checking built into UltraCAS prevent the Set Top Box media pipeline from being compromised.

The next section of the MovieLabs specification is referred to as "**DRM System Specifications"**.

MovieLabs spec: **DRM System Specifications**

MovieLabs spec: Cryptography

- The system shall use state of the art cryptographic functions, e.g., a cipher of AES 128 or better.

UltraCAS goes beyond AES and other state of the art with a FIPS 140-2 certified Crypto Core. The minimum security level for UltraCAS is based on state of the art cryptographic functions including AES 128, 2048 bit RSA, SHA-256 and other equally state of the art crypto functions. In addition to the crypto functions, the run time firmware integrity checking, secure boot, active Hacker detection, and other firmware protection levels are as important, or in-fact are more important than using state of the art cryptographic functions. This is because if a hacker can easily access a key the strongest crypto function does not provide any protection for an exposed key. Key protection is requirement of the CAS system and UltraCAS uses all available embedded keys with a quickly renewed security client providing excellent security on top of incorporating state of the art crypto functions.

MovieLabs spec: **Side Channel Attacks**

The system shall be resistant to side channel attacks, including but not limited to timing attacks, simple power analysis (SPA), differential power analysis (DPA), simple electro-magnetic analysis (SEMA), and differential electro-magnetic analysis (DEMA), that utilize a commercially viable level of effort, e.g., number of traces. The resistance shall be established through testing, e.g., through statistical analysis of test signals for leakage.

Side Channel Attack security is in the domain of the Set Top Box chip provider and Secure TV can help its customers select hardware that meets the Hollywood Studios and the MovieLabs specification for hardware based Side Channel Attacks.

MovieLabs spec: **Connection**

The system shall allow the content provider to hold back the delivery of license keys to the device until the street date.

UltraCAS for IPTV includes FIPS 140-2 Certified software, a TSL/SSL protection communication path with TSL/SSL protected key exchange with license keys that are protected in the same way e-commerce and online banking transactions are protection. Content street date data is part of the SSL protected key exchange data.

MovieLabs spec: **Copy or Move**

Systems supporting copy or move shall require the license to be re-provisioned through an on-line process that is performed using keys not present on client devices after a copy or move

UltraCAS supports this requirements in that license keys are never copied, moved, or exposed. In addition, license keys are bound to a hardware device keyset. In the unlikely event that keys were copied the keys are not appropriated for a different device because keys are bound to hardware chip specific data.

MovieLabs spec: **Hack One, Only Hack One**

The compromise of security on one platform shall be limited to that platform. And the compromise of security on one distribution of a title shall be limited to that distribution.

UltraCAS incorporates numerous levels of hardware binding, server side active network probing, IP related active network probing, and client software hardware binding that independently isolate devices at multiple layers. Because of the layered security approach, in the unlikely event of a device hack the hack will only be isolated to only that device, and if the cloned device is used to access content the active network probing software on the server will detect the clone accessing the network.

MovieLabs spec: **Binding to Device**

The system shall bind the ability to decrypt a license key to a particular device (host and/or storage). License keys shall be encrypted such that they cannot be decrypted without the keys of the individual device for which the license was issued.

UltraCAS excels in device binding using a combination of hardware provisioned keys, device unique license keys bound to hardware IDs, along with device network binding that includes active network probing. License keys are encrypted for only a single device using multiple device specific IDs and delivery is monitored to detect clone devices attempting access from different IP addresses. In addition, run-time integrity code checking that is dynamically updated detects tampered software.

MovieLabs spec: **Key compromise**

The compromise of the keys for a set of devices shall not make it easier to derive the keys for another device.

As discussed in earlier sections, UltraCAS excels in preventing key compromise as explained in the previous section on “Binding to Device”. In addition, keys are bound to a hardware device keyset. In the unlikely event that keys were copied the keys are not appropriated for a different device because keys are bound to hardware chip specific data. While anything can be cloned however difficult, and cloning a STB chip keyset and software key set is extremely extremely difficult, active network probing will detects clones preventing keys from being used by another device.

MovieLabs spec: **Software Diversity**

Security related software shall be implemented in diverse ways so that an attack is unlikely to be portable. This diversity shall vary by version of the system and by platform.

UltraCAS includes many layers of software diversity preventing attacks from being portable including using UltraCAS secure hardware key drivers that use secure silicon keys contained in Set Top Box chips, with hardware binding key processing that incorporates hardware specific data into the key processing, coupled with active network probing, and Rapid Security Software Renewal (RSSR) that changes the entire client security software on a frequent basis forcing hackers to have to continuously hack the system, something that will discourage the hacking attempts. Rapid Security Software Renewal can be equated to Greek mythology where Sisyphus was cursed to push a boulder up a hill and watch it go down eternally. Hackers attempting to hack the system will be cursed to have to keep up with the Rapid Security Software Renewal built into UltraCAS.

MovieLabs spec: **Copy Title Diversity**

The content protection system shall provide capabilities so that in the event of a breach on one title or version of a title, additional work is needed to breach the content protection on the next title or another version. (N.B., simply using different content keys is not sufficient to satisfy this practice.).

UltraCAS has perhaps the most innovative security for MovieLabs Copy Title Diversity. In fact, UltraCAS's Copy Title Diversity is so unique Secure TV provides details only after an NDA is signed. Rest assured that the Secure TV security in this area like other security processing is industry leading.

MovieLabs spec: Integrity Robustness

Runtime integrity checking of the DRM system must be performed either by the DRM system or by the platform.

UltraCAS not only uses the DRM system and platform, but also uses the network to ensure the Integrity of the system providing Robustness beyond our competitors. The UltraCAS Secure Hardware Drivers use the hardware security built into the latest Set Top Box chips. In addition, software run-time integrity checking dynamically monitors for code changes as well as debugger insertions. Finally, real-time active network probing detects clones based on network monitoring on the server side outside the reach of hackers.

MovieLabs spec: **Isolation and Trust**

The system shall use the platform isolation and trust mechanisms specified in the Platform Specification section below.

UltraCAS complies with the Platform Isolation and trust Specifications described in more detail below.

MovieLabs spec: **Revocation and Renewal**

The system shall have the ability to revoke and renew versions of its client component.

UltraCAS has been designed and built on the premise that renewability and revocation provide the last line of defense against hacker attacking the system. The reason for this is because anything digital can be hacked, and while the current day Set Top Box chips and client software are extremely difficult to hack, it is not impossible. In the very unlikely event of a hack, the only defense is to renew the clients and revoke known clones attempting to steal the Pay TV service.

This portion of the response is copied from the "Software Diversity" section above: UltraCAS includes many layers of software diversity preventing attacks from being portable including using UltraCAS secure hardware key drivers that use secure silicon keys contained in Set Top Box chips, with hardware binding key processing that incorporates hardware specific data into the key processing, coupled with active network probing, and Rapid Security Software Renewal (RSSR) that changes the entire client security software on a frequent basis forcing hackers to have to continuously hack the system, something that will discourage the hacking attempts. Rapid Security Software Renewal can be equated to Greek mythology where Sisyphus was cursed to push a boulder up a hill and watch it go down eternally. Hackers attempting to hack the system will be cursed to have to keep up with the Rapid Security Software Renewal built into UltraCAS.

MovieLabs spec: **Revocation and Renewal – Code Signing Certificates**

The system shall have the ability to revoke subsidiary code signing certificates if these are used as part of the system's root of trust.

Set Top Box client code signing certificates are part of the systems root of trust and are revocable in the UltraCAS system. By design, the certificate hierarchy in the UltraCAS system completely isolates each Pay TV operator as a result of each operator having their own root signing certificate not shared with

other operators. In addition, the root signing certificate can be revoked or renewed if necessary over-the-air without the need for a service truck roll.

MovieLabs spec: **Revocation and Renewal – devices or classes**

The system shall have the ability to revoke individual devices or classes of devices.

ltraCAS has built in support to revoke individual devices or classes of devices such as Android Mobile Phones, or a certain model of Set Top Boxes. Devices are classified by type (Set Top Box, Mobile Phone, Tablet, Laptop, etc.), as well as by Manufacturer and either category of device type or manufacturer can be revoked. More importantly, after revocation individual devices from any revoked class can be reactivated so only compromised devices are revoked in a class.

MovieLabs spec: **Proactive renewal**

The system shall proactively renew its security related software components.

UltraCAS incorporates a Proactive Renewal updating system for its security client using a Secure TV security tool called *CryptoBuilder.* CryptoBuilder is an automated security software tool that builds an unlimited number of cryptographically secure security client libraries that are used to proactively renew the security related software components.

UltraCAS includes server-side active breach monitoring detecting cloned devices when the cloned device attempts to access the network using IP network probing. On one-way networks, Secure TV monitors hacker forums as well as monitoring sites that sell universal pirate Set Top Boxes.

MovieLabs spec: **Outputs: Link Protection**

- The system shall support the requirement of HDCP 2.2 or better for specific content types, e.g., Ultra HD or enhanced HD.

Supported with combination of UltraCAS and STB chip

- The system shall support the requirement of HDCP 2.2 or better by the content provider, e.g., in the license.

Supported with combination of UltraCAS and STB chip

- The system shall allow other available outputs and their associated protection to be selectable by the content provider, e.g., in the license.

Supported with combination of UltraCAS and STB chip

For the "Outputs: Link Protection" requirements UltraCAS passes license related output control data to the HDCP control registers in the Set Top Box Chip.

MovieLabs spec: **Encryption**

The platform shall support a content cipher of AES 128 or better.

Supported. UltraCAS uses AES 128.

- The platform shall provide the support necessary to make a DRM system resistant to side channel attacks as specified in the DRM section above.

Supported as described in the DRM section above.

- The platform shall support a random number generator compliant with NIST 800-90C.

UltraCAS uses a NIST compliant Random Number Generator

MovieLabs spec: **Secure Media Pipeline**

The platform shall implement a secure media pipeline that provides end to end protection that encompasses, at a minimum, decryption through to protected output.

Supported in UltraCAS with protected media path as described above.

This secure media pipeline shall include protecting secrets (including keys and derivative key material)

Supported in UltraCAS with hardware protected keys in secure silicon for the secure media pipeline

and both compressed and decompressed video samples from access by any non-authorized source using the isolation and trust mechanisms described below.

Supported in UltraCAS with HDCP protected outputs, secure boot, debugger detection, code modification detection as part of run-time integrity checking.

MovieLabs spec: **Secure Computation Environment**

- The platform shall support a secure processing environment isolated by hardware mechanisms running only authenticated code for performing critical operations. The security of this environment must have been proven with extensive testing.

UltraCAS supports this requirement with a secure protected processing environment running on isolated hardware for performing critical CAS operations.

o E.g., secure OS, media pipeline configuration, handling sensitive cryptography

Supported with secure boot, run-time integrity checking, secure media pipeline configuration, and hardware based sensitive key cryptographic processing.

- The platform shall be able to protect memory of the secure execution environment against access from untrusted code & devices.

Supported in UltraCAS with secure boot, run-time integrity checking, secure media pipeline configuration, and protected output paths as described.

- The platform should support runtime integrity checking of secure applications.

Supported in UltraCAS with secure boot, debugger detection, code modification detection as part of run-time integrity checking.

MovieLabs spec: **Hardware Root of Trust**

- The platform shall support a secure chain of trust for code that executes in the secure execution environment.

Supported in UltraCAS with secure boot and run-time integrity checking as described above.

The root of this trust shall be securely provisioned, e.g., permanently factory burned.

Supported in UltraCAS with silicon protected keys permanently burned at factory, and silicon protected secure boot.

- The platform shall provide a secure mechanism for DRM systems to store secrets in local, persistent storage in a form encrypted uniquely for the device and, if the platform supports multiple trusted applications or DRMs, uniquely for each in a way that securely prevents a trusted application from decrypting the secrets of others. The encryption must be rooted in a secret, immutable, device unique value with at least 128 bits of entropy.

Supported in UltraCAS as described above. Encryption root is a secret, immutable, and device unique value with 128 bits of entropy stored in secure silicon in the chip.

MovieLabs spec: **Link Control/Protection**

- The platform shall support HDCP 2.2 or better on all HDCP protectable outputs.

Supported in UltraCAS controlling STB with HDCP 2.2

- Devices with HDCP protectable inputs, e.g., displays and receivers, shall support HDCP 2.2.

Supported in UltraCAS controlling STB with HDCP 2.2

- The platform shall secure output selection so that only authorized code can enable other outputs.

Supported in UltraCAS controlling STB with HDCP 2.2 with secure boot protection, run-time integrity checking, and secure control on HDCP control bits.

- The platform should support runtime integrity checking of secure applications.

Supported in UltraCAS with secure boot, debugger detection, code modification detection as part of run-time integrity checking.

MovieLabs End-to-End System Specifications

MovieLabs spec: **Forensic*Watermarking**

- The system shall have the ability to securely forensically mark video at the server and/or client to recover information necessary to address breaches.

This support will be added enabling a 3rd party forensic watermark running on the Set Top Box SOC chip. Different STB chips have integrated different watermarking schemes from watermark software providers.

- The watermarking shall be robust against corruption of the forensic information.

This support will be added enabling a 3rd party forensic watermark running on the Set Top Box SOC chip.

- The watermark shall be inserted on the server or on the client such that the valid insertion is guaranteed during playback even if the device and its secrets are compromised.

This support will be added enabling a 3rd party forensic watermark running on the Set Top Box SOC chip.

MovieLabs spec: **Playback*Control Watermark**

- A compliant system shall implement Cinavia playback

k controls on all content.

MovieLabs requires "Processes and agreements shall be in place to enable rapid response in renewing any compromised software component of the system." UltraCAS supports this requirement with production ready security system software ready to be deployed in the unlikey event of the system being compromised.

Certification

On page 6 in Certification, MovieLabs requires: "The compliance of the system and the robustness of its implementation shall be certified by a combination of 3rd parties and trusted implementers." The current version of SecureTV 3.0 has been certified by both Merdan and the Independent Security Evaluators (ISE). UltraCAS being an upgrade to SecureTV 3.0 shall be independently certified by a Hollywood trusted 3rd party.

For completeness the following section is copied from the last page of the MovieLabs 1.1 specification:

- Prior to certification, the number of devices that can decrypt production titles shall be securely limited to a small number. While not a requirement, this feature is supported by only securely provisioning a small number of devices.

- Development code shall be securely prevented from running on production units, e.g., by revoking the signing certificate or by using a different root certificate and hardware root of trust. Supported in UltraCAS.

- Production code shall limit, to the extent technically feasible, any information that could be useful to reverse engineering, such as debugging, tracing, or symbolic information. Supported by restricted access secure software development area with software development on machines that do not have Internet connects, very limited distribution of technical information as well as spreading printouts.

Conclusion

As one can see from the above detailed breakdown, UltraCAS meets and exceeds the requirements set forth in the MovieLabs Specification for Enhanced Content Protection v1.1 dated February 2015. Each and every requirement set out by MovieLabs has been presented along with an explaining detailing the superior CAS features incorporated into UltraCAS.