PROMETHEUS
SECURITY GROUP GLOBAL

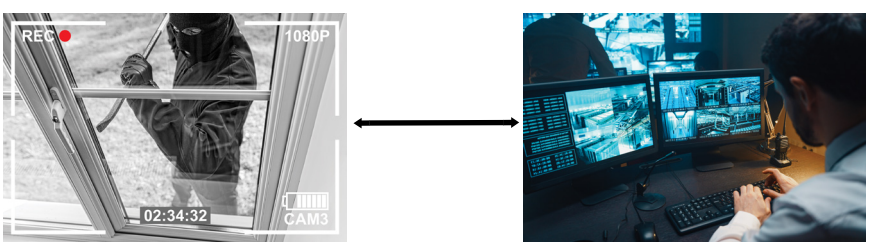
SCENE AUTHENTICATION

SAFE | SECURE | CERTIFIED

Product Overview

Scene Authentication that validates the video data from the scene viewed by the camera through its storage. Scene Authentication uses a unique technology to watermark the camera's field of view and, using standards based cryptography, continuously verify the integrity of the scene in real-time through transmission, storage and display. Scene Authentication ensures that video is live, authentic and not manipulated in real-time. The technology deploys in the scene viewed by a camera, an encrypted light source called an Authentication Information Transmitter (AITX). The AITX continuously outputs an encrypted timestamp that is continually monitored by a paired receiver (Authenticator algorithm).

The Authenticator can be deployed at various points in the system. For example, a video recorder may implement the Authenticator to alert of any hacking or tampering of the video feed. The Authenticator is used during forensics to validate the time of the video.



Features	Benefits
U.S. Patent Aug 2016	Unique end-to-end protection
AES Encryption and RSA Signing	Advanced encryption and protection
Automated Pairing and Tuning Algorithm	Easy installation and configuration
Configurable Alerting	Differentiates a real attack from an interruption
Environmental Tuning	Reduces False Positives
Aware of time, spatial positioning	Verifies Video Veracity
Metadata Validation	Protects stored video with reversible audit
Integrated with ONVIF	FIPS-140-2
Available for OEM Integration	Technology can be integrated into camera/encoder firmware
USB Host One to Many Programming	Manage many devices from a single secure token
Industrially Designed	-40° to +70° C operation, made for uptime and reliability

512.247.3700 | sales@psgglobal.net www.psgglobal.net

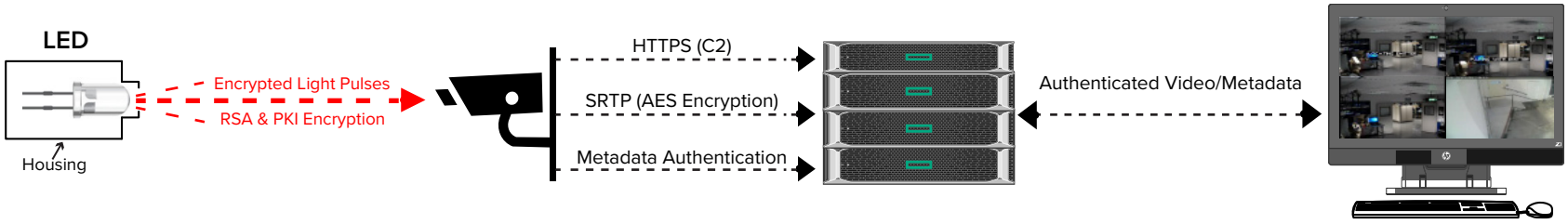
PROMETHEUS
SECURITY GROUP GLOBAL

Active Transmitter in Field of View

Surveillance Camera

HPC

Viewer



- Supplies encrypted coded light signal
- Signal placed in the video scene
- Signal supplies geo-coordinates of emitter
- Spatial Location within video scene & time
- Public key loaded on emitter via USB
- PKI encryption secures data as transmitted
- Up to 4 emitters in a scene
- Tamper protected housing

- Compliant with USAFI 31-101/AFMAN Section 9.15.3 regarding spoofing, bypassing, or system sabotage
- Receiver Software decrypts emitter metadata
- Detects Video Loops
- Detects covering of the emitter
- Detects injected video
- RSA signed data

- Decodes authentication signal
- Sends authentication metadata to storage
- Alerts guard of tampering
- Receiver software is a part of VICADS

- Authenticated Video from scene to viewer
- Emitter signal is masked out of the operator view

Acronyms:
- RSA Encryption - Asymmetric private / public key encryption
- PKI - Public Key Infrastructure to authenticate users and devices
- SRTP – Secure Real Time Protocol (AES Encryption for video)

Legend:
Red = Encrypted light from emitter
Black = Authenticated Video/Metadata over IP

512.247.3700 |
sales@psgglobal.net
www.psgglobal.net