

## Converging Physical Security with Zero Trust

*"EDGE to Enterprise and beyond"*

### SCENE AUTHENTICATION

#### Product Overview

Scene Authentication is a PSG Patented product which provides real-time authentication of a video signal from its inception (video scene) to its delivery (viewing or storing). It is the first end-to-end authentication of its kind and simultaneously protects video signaling from spoofing, tampering and hijacking. Scene Authentication assures users that any instances of video produced by their surveillance system came from its cameras, at that the actual location at a specified point in time.

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	- Federal Information Processing Standard (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

# Converging Physical Security with Zero Trust

*"EDGE to Enterprise and beyond"*

## Emitter



PKIE ncrypted  
LightP ulses

0 0 0 0 0 0 0 0 0 0  
1 1 1 1 1 1 1 1 1 1  
0 1 0 0 1 0 1 0 0 1

- 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 when transmitted
- Up to 4 emitters in a scene
- Tamper protected housing

## Camera/Sensor



Encrypted Network Communication

0  
1  
0 1 0 0 0 0 0 1 0 0 0 0 0 0 0 1 0 0 0 1

- Receiver Software decrypts emitter metadata
- Detects Video Loops
- Detects covering of the emitter
- Detects injected video
- RSA signed data
- HTTPS (C2)
- SRTP (AES Encryption)

## Viewer



- Authenticated Video from scene to viewer
- Emitter signal is masked out of the operator view
- Decodes authentication signal
- Sends authentication metadata to storage
- Alerts guard of tampering
- Receiver software is a part of VICADS