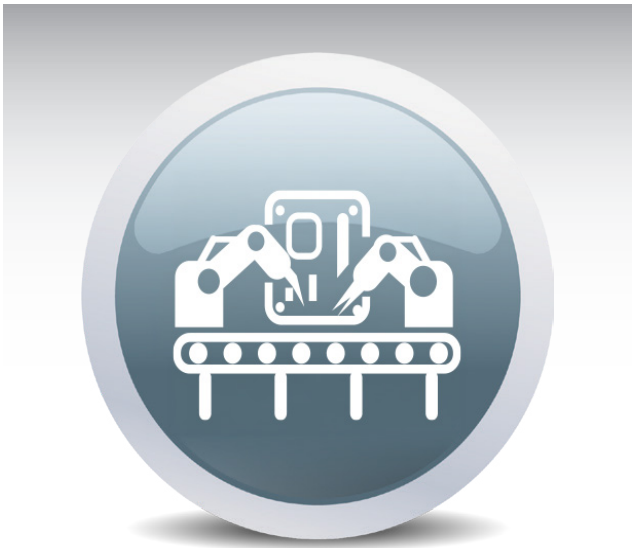
DPX® Media Validation Toolkit

Firmware-Level Media Integrity Framework for DPX Gaming Platforms



Features

Firmware-Level Media Validation
- Pre-boot verification of operating system and game content on SATA, NVMe, or USB media
- Deterministic enforcement during system initialization
- Prevention of execution of unauthorized or modified software

Cryptographic Integrity Framework
- UEFI-based validation integrated within platform firmware
- Support for configurable cryptographic hash mechanisms
- Hash support SHA -256 and SHA-160
- Compatibility with GPT and legacy boot configurations

Hardware and Software Binding
- Controlled association between approved system media and designated hardware platforms
- Encrypted hash digest
- Multi-game support

Field proven and approved by GLI, NVGCB and other global regulatory agencies

Windows Linux

Introduction

The Media Validation Toolkit (MVTK) provides a firmware-integrated integrity framework for validating boot media and system software components on DPX gaming platforms. Operating at the UEFI (BIOS) layer during system initialization, MVTK verifies operating system and game content stored on approved media before execution. Only validated and authorized software is permitted to run.

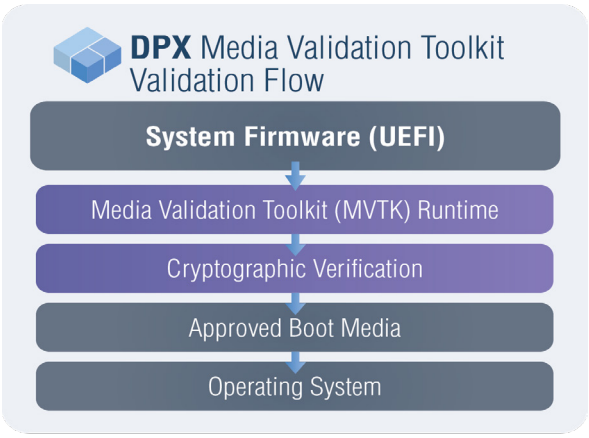
MVTK is designed to support media validation requirements in regulated gaming jurisdictions, including U.S. and international regulatory frameworks.

MVTK is available for supported DPX platforms.

Architecture & Capabilities

MVTK operates within system firmware before operating system handoff. During initialization, it validates approved boot media using platform-managed verification data. Validation decisions are enforced deterministically, ensuring consistent behaviour across development, certification, and production environments.

The architecture is designed to:
- Validate all critical control program software before execution
- Generate and verify SHA-based hashes to detect unauthorised or corrupted software
- Establish a secure chain of trust from system firmware through to validated software
- Prevent unauthorised or modified software from executing
- Support software integrity and authentication requirements for regulated gaming environments



DPX-Media Validation Toolkit

Package Contents

The MVTK package includes:	Firmware-integrated validation framework
	Configuration and provisioning utilities (where applicable)
	Developer documentation

System Requirements

Development Environment	Supported Windows and Linux operating systems aligned with the selected DPX platform
	Access to platform firmware configuration mechanisms
Target Platform	Supported DPX Series motherboard or integrated system
	Compatible platform firmware and BIOS configuration

Integration & Compatibility

MVTK integrates with:

- DPX Gaming Platform Security Architecture (GPSA)

This layered architecture ensures consistent integrity enforcement across supported DPX platforms

MVTK functions as part of the platform integrity layer and operates independently of application software once enforcement is enable

It maintains consistent validation behavior across supported platforms and supports long lifecycle deployments typical of regulated gaming markets.

Benefits

- Establishes controlled validation of boot media
- Enforces deterministic platform integrity during system initialization
- Supports hardware and software configuration binding
- Aligns with regulatory validation processes
- Maintains consistency across long lifecycle platform deployments

OEM Customization and Product Development

Advantech Gaming Solutions provides PC-based hardware and software design services for regulated gaming applications, supporting customized platform development and long-term product lifecycle management.