CommScope Launches Secure Boot Solution for Texas Instruments' Arm-based AM6x Processors

Jan 06, 2026

CommScope PRiSM, with hardware-backed signing and automated workflows, reduces development effort and accelerates compliance with the EU Cyber Resilience Act

RICHARDSON, Texas--(BUSINESS WIRE)--Jan. 6, 2026-- CommScope (NASDAQ: COMM), a global leader in network connectivity, today announced a fully tested, out-of-the-box bootloader signing solution for the Texas Instruments' (TI) Arm-based AM6x processor family. Built on CommScope's PRiSM™ (Permission Rights Signing Manager) platform, this solution is simple and easy to integrate with the TI image build process; and it ensures robust key protection using a FIPS-certified Hardware Security Module (HSM) and centralized key lifecycle management. The solution delivers a production-ready path to secure boot adoption—streamlining Continuous Integration/Continuous Delivery (CI/CD) and meeting cybersecurity mandates without requiring teams to build and manage their own cryptographic infrastructure.

"Secure boot is a cornerstone of system integrity and robust protection against software tampering," said Sonia Ghelani, Product Line Manager, Sitara™ Processors, Texas Instruments. "With CommScope's production-grade infrastructure and HSM-protected signing keys, we're enabling customers to fully leverage TI's security capabilities, which help simplify secure boot adoption and defend against today's sophisticated cyberattacks."

Bootloader security is a critical foundation for ensuring device integrity because it determines whether firmware can be trusted before executing it. This function requires protecting the private signing key used to authenticate firmware; if that key is compromised, even secure boot mechanisms can be bypassed. CommScope's solution helps manufacturers safeguard this key with hardware-backed security and controlled access, offering a clear, auditable path to meet emerging cybersecurity mandates, including the European Union's Cyber Resilience Act (CRA) as well as other regional and industry-specific standards.

"Security should never be a barrier to product innovation," said Craig Coogan, CTO & VP, Product & Strategy, Access Network Solutions, CommScope. "By collaborating with TI, we help device makers simplify secure boot adoption, reduce development friction, and deliver trusted products into regulated markets with confidence. We handle the underlying complexity so device manufacturers can focus on what they do best to improve productivity, streamline development, and strengthen security outcomes."

CommScope® PRiSM Benefits

- **Full, Robust Key Lifecycle Protection**: Signing keys are generated through a multi-party-controlled process, deployed into FIPS-certified HSMs, and never exposed in software. Their full lifecycle—from creation to controlled use—is tightly managed to prevent key leakage, unauthorized access, or malicious replacement—any of which could compromise the integrity of secure boot.
- **Strict Access Control and Policy Enforcement**: Enforce security policies that restrict signing operations to approved entities with role-based access controls (RBAC) and eTokens for authorized users and build systems. This minimizes the risk of unauthorized use, insider threats, and policy violations during image signing.
- **Seamless CI/CD Integration**: The PRiSM platform provides a secure, cloud-accessible API integrated with TI's software development kit (SDK), enabling scalable and automated signing workflows that don't disrupt development pipelines.
- **Comprehensive Visibility and Auditability**: The PRiSM platform maintains a full audit trail of all signing operations, capturing who signed what, when, and from where. This supports both internal accountability and external compliance requirements.

Availability & Resources

"The CommScope secure boot package will be available in Q1 2026. TI AM6x customers may request onboarding details through our TI partner page, here you will also find comprehensive recorded walkthroughs and personalized support resources. For general information regarding our security solutions, please visit the CommScope PKI Center website."

CommScope and the CommScope logo are registered trademarks of CommScope and/or its affiliates in the U.S. and other countries. For additional trademark information see https://www.commscope.com/trademarks. Sitara is a trademark of Texas Instruments Incorporated. All other product names, trademarks and registered trademarks are property of their respective owners.

About CommScope:

CommScope (NASDAQ: COMM) is pushing the boundaries of technology to create the world's most advanced wired and wireless networks. Our global team of employees, innovators and technologists empower customers to anticipate what's next and invent what's possible. Discover more at www.commscope.com.

Follow us on LinkedIn and X. Sign up for our press releases and blog posts.

This press release includes forward-looking statements that are based on information currently available to management, management's beliefs, as

well as on a number of assumptions concerning future events. Forward-looking statements are not a guarantee of performance and are subject to a number of uncertainties and other factors, which could cause the actual results to differ materially from those currently expected. In providing forward-looking statements, the company does not intend, and is not undertaking any obligation or duty, to update these statements as a result of new information, future events or otherwise.

Source: CommScope

View source version on businesswire.com: https://www.businesswire.com/news/home/20260106728043/en/

News Media Contact:
Luke Hamer
Luke.Hamer@commscope.com

Financial Contact:
Massimo Disabato, CommScope
Massimo.Disabato@commscope.com

Source: CommScope