tetrate

Zero Trust, FIPS and FedRAMP for Cloud-Native Applications

Tetrate's FIPS-verified distribution of Istio is designed for organizations requiring FedRAMP authorization—including FedRAMP Rev. 5

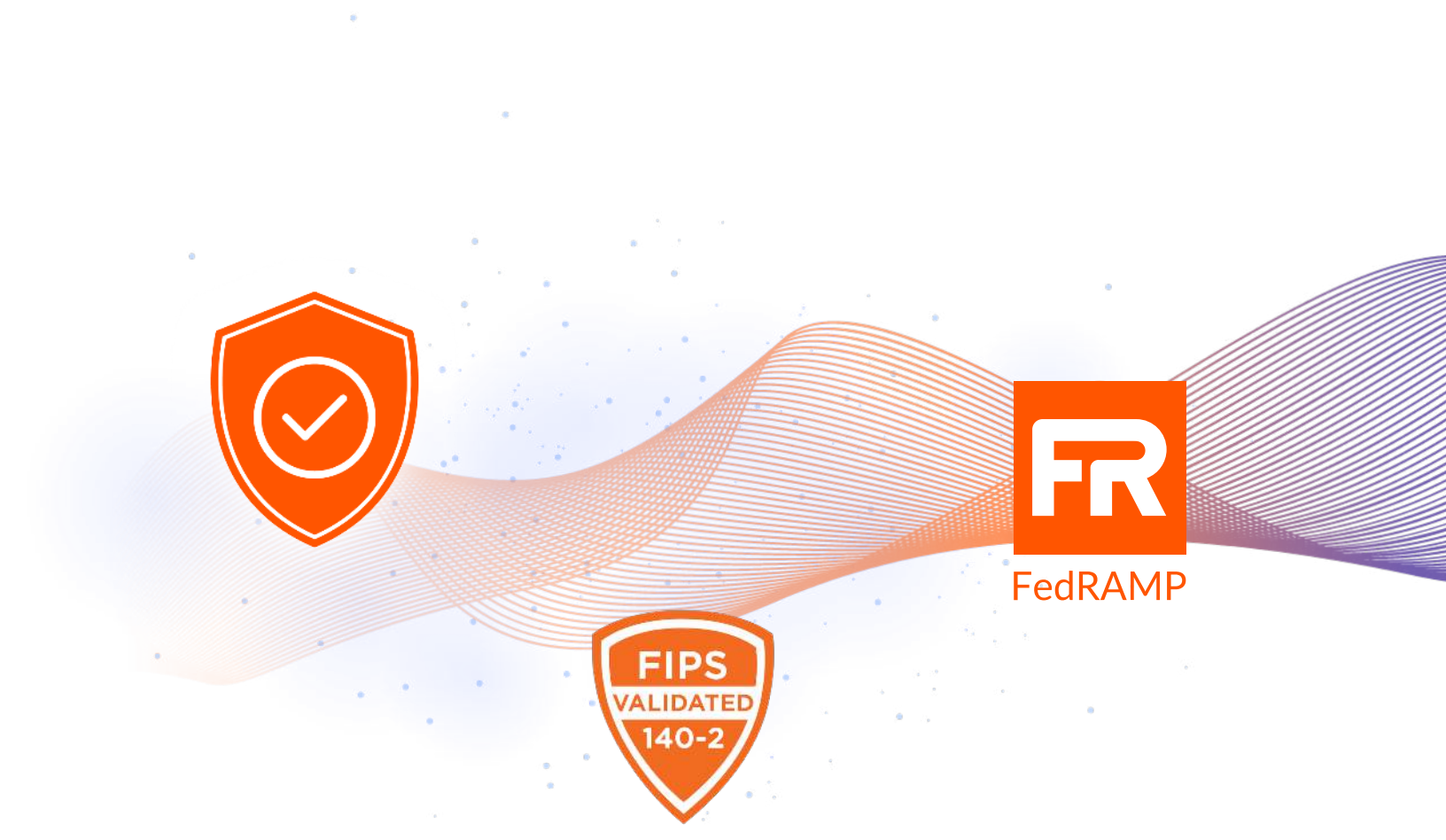

Table of Contents

Executive Summary

FedRAMP and FIPS validation are important for ensuring the security, compliance and risk management of cloud products and services used by government agencies and organizations in highly regulated environments. They provide a standardized framework for security assessment and authorization, as well as cryptographic standards for data encryption, reducing the risk of security incidents and unauthorized access to information.

Tetrate offers a FIPS-verified distribution of Istio specifically designed for organizations requiring FedRAMP authorization - including FedRAMP Rev. 5. A FIPS compliant build of Istio can help you achieve compliance, accelerate your FedRAMP approval process and ensure applications are protected.

This primer will help you better understand FIPS and FedRamp for cloud-native applications and provides deeper insight into key issues including:

- Enterprise information security architecture has become increasingly important as information systems have evolved into critical business assets.
- Zero trust network architecture is emerging as a preferred approach for enterprises to secure both their traditional and modern, cloud-native applications. A key component of zero trust architecture is encryption in transit.
- The Istio service mesh acts as a security kernel for distributed applications and serves as the foundation of a zero trust architecture, including providing comprehensive encryption in transit between system components.
- Tetrate offers a FIPS-verified distribution of Istio specifically designed for organizations requiring FedRAMP authorization—including FedRAMP Rev. 5—and other organizations in regulated environments where the stock builds of Istio and Envoy aren't suitable.
- The Federal Information Processing Standards (FIPS) are the information security standards for the U.S. federal government. Information systems built and run by federal agencies, contractors, and vendors are required to adhere to FIPS.
- FIPS is also widely regarded as a set of robust and trustworthy security standards that is often adopted by private sector organizations.
- The National Institute of Standards and Technology (NIST), the standards body responsible for defining FIPS, runs a program (CMVP) to validate that cryptographic modules adhere to FIPS standards and are suitable for use in U.S. federal agency information systems. Those modules are said to be FIPS validated. Software certified by a CMVP-accredited laboratory as using FIPS-validated modules correctly is said to be FIPS verified.
- Tetrate offers a 100% upstream distribution of Istio and Envoy called Tetrate Istio Distro (TID) that is the first to be FIPS verified.

Why Information Security Architecture Is Important

Information security architecture has become increasingly important as information systems have evolved into critical business assets. Cyber crime has reached industrial scale at the same time that business-critical functionality is growing more sophisticated and powerful.

That power comes with greater complexity: there are more pieces and parts that need to communicate with each other over networks and more places where those components and users can operate outside the traditional data center and fortified network perimeter. These pieces, parts, people, places - and their access to each other - must all be secured.

Traditional security architecture has long followed the paradigm of a strong fortified perimeter with more permissive access to internal systems once a user has been authenticated, authorized and let through the castle gates.

The complexity of modern, cloud-native applications and associated risk to critical business assets and reputation has prompted many organizations (and the U.S. federal government) to re-think their information security architecture from the ground up.

Zero Trust Architecture Is the Future of Enterprise Network Security

Traditional network security relies on a strong defensive perimeter around a trusted internal network to keep bad actors out and sensitive data in. In an increasingly complex networking environment, maintaining a robust perimeter is increasingly difficult.

Zero trust network architecture is emerging as a preferred approach for enterprises to secure both their traditional and modern, cloud-native applications. Zero trust network architecture inverts the assumptions of perimeter security. In a zero trust network, every resource is protected internally as if it were exposed to the open internet.

Zack Butcher, Tetrate founding engineer and co-author of the NIST standards for microservices security, identifies the following minimum five core runtime requirements for a zero trust architecture:

1. Communication within the system, with end-users, and with external systems should be encrypted (also known as encryption in transit) to ensure authenticity, integrity, and privacy;
2. All service-to-service communication should be mutually authenticated;

3. All service-to-service communication should be mutually authorized;
4. All end-user communication should be authenticated;
5. All end-user communication should be authorized.

As a dedicated infrastructure layer, the Istio service mesh acts as a security kernel for distributed applications that satisfies all five of these requirements. When we're talking about FIPS, we're solely focused on the first requirement: encryption in transit.

Istio and Zero Trust in a FedRAMP Environment

What Is FedRAMP?

The Federal Risk and Authorization Management Program (FedRAMP) is a U.S. government-wide program that standardizes the security assessment, authorization and continuous monitoring processes for cloud products and services used by federal agencies. FedRAMP was established to ensure that cloud solutions meet specific security requirements and standards to protect sensitive government data.

Cloud service providers (CSPs) seeking to work with federal agencies must go through a rigorous assessment and authorization process to achieve a FedRAMP Authorization. This process involves a comprehensive security evaluation and documentation of how the cloud service meets specific security controls and requirements.

Once a cloud service has been granted a FedRAMP Authorization, it means that it has met the security standards required to serve federal government agencies, making it easier for agencies to adopt and use these cloud services while maintaining data security and compliance. FedRAMP helps ensure the protection of sensitive government information while promoting the adoption of modern cloud technologies within the federal government.

FedRAMP and NIST SP 800-53

FedRAMP builds upon the security standards established by the National Institute of Standards and Technology (NIST) in its Special Publication (SP) 800-53. NIST SP 800-53 provides a comprehensive catalog of security controls and control enhancements that federal agencies can use to secure their information systems and protect sensitive data.

FedRAMP takes the security controls from NIST SP 800-53 and provides a framework for how CSPs should implement them in the context of cloud services. When a cloud service provider achieves FedRAMP Authorization, it means that their cloud offering has been assessed and found to comply with the specific security requirements outlined in both NIST SP 800-53 and FedRAMP.

FedRAMP Is Now Law

In December 2022, the FedRAMP Authorization Act was signed as part of the FY23 National Defense Authorization Act (NDAA). The Act codifies the FedRAMP program as the authoritative standardized approach to security assessment and authorization for cloud computing products and services that process unclassified federal information.

What's New in FedRAMP Rev. 5

There are different revisions of NIST SP 800-53, with each revision introducing updates and improvements to the security controls framework. The latest revision, Rev. 5, finalized in 2020, applies to new FedRAMP authorizations starting May 30, 2023.

Broadly, here's what's new in Rev. 5:

- **Expansion to 20 control families** (from 18 in Rev. 4), with some controls being restructured and renumbered. The control families are also realigned to better match current security threats and technology trends. (For more information, see Tetrate's Guide to FedRAMP Rev. 5.)
- **Expansion of scope to include privacy controls** in addition to security controls to reflect the growing importance of privacy protection in information systems.
- **Greater emphasis on supply chain risk management** and includes controls related to software supply chain security, reflecting the increasing importance of securing the software development and distribution process.
- **Better alignment with other cybersecurity and privacy frameworks** such as NIST's Cybersecurity Framework (CSF) and Privacy Framework.
- **Increased Emphasis on continuous monitoring and improvement** of security and privacy controls, aligning with modern cybersecurity practices.

Note: FedRAMP authorizations already in the initiation or continuous monitoring phase prior to May 30, 2023 may continue to use Rev. 4 baselines, but must identify the delta between their current Rev. 4 implementation and the Rev. 5 requirements plus develop plans to address that delta.

Tetrate Istio Is the Fastest Way to FedRAMP ATO (Including Rev. 5)

FedRAMP Rev. 5 requires FIPS-validated encryption for data in transit. While Istio is the de facto standard security kernel for microservices applications, only Tetrate offers a FIPS-validated distribution of Istio suitable for FedRAMP environments. New in FedRAMP Rev. 5 is a requirement to document cryptographic modules in use to protect data in transit and at rest. Tetrate's Istio distribution is built into the documentation template (SSP Appendix Q) required for all System Security Plans (SSPs)—so, you can be sure when it's time to pass the Full Security Assessment in the FedRAMP Authorization phase , Tetrate has you covered. Tetrate Istio is also available via approved software factories like the AWS Marketplace for GovCloud and Platform One.

What Is FIPS?

FIPS is a set of standards for information processing systems that all U.S. federal agencies, contractors, and vendors must adhere to. FIPS is also widely regarded as a set of robust and trustworthy security standards that is often adopted by private sector organizations.

A key part of FIPS governs cryptographic modules, the specialized hardware, software, and/or firmware that encrypt data to ensure privacy and authenticity. NIST offers a validation program for cryptographic modules to ensure that validated modules are safe and approved for use in federal information systems.

FIPS. Federal Information Processing Standards are the information security standards for the federal government defined by the National Institute of Standards and Technology (NIST) in accordance with the Federal Information Security Management Act (FISMA). As part of FIPS, the standards for cryptography are evolving, with the FIPS 140-2 document currently in effect and FIPS 140-3 published but not yet required by authorizing officials (AOs), the officials who grant authorization to operate (ATO), which is required to run any software for government use.

CMVP. The Cryptographic Module Validation Program (CMVP), a joint effort between NIST and the Canadian Centre for Cyber Security, promotes the use of validated cryptographic modules. CMVP tracks crypto implementations that have been validated by auditors to conform to FIPS 140-2 and/or 140-3.

FedRAMP. FedRAMP, the most common ATO in the U.S. government, requires the use of FIPS 140-2 validated modules for encrypting data in transit and at rest.

What Is FIPS *Validated* vs *Verified* vs *Certified*?

FIPS validation. As part of CMVP, NIST authorizes independent labs to audit cryptographic modules submitted for review. Modules that pass this review are said to be **FIPS *validated***. The validation status of all modules submitted to CMVP is published via a publicly searchable database.

FIPS verification. Software that uses FIPS-validated cryptographic modules may need additional verification from an accredited testing lab that those cryptographic modules are used correctly in order to be authorized by a program like FedRAMP. Such software is said to be **FIPS *verified***.

This approach to achieving federal authorization is a safer alternative to forking a module for independent FIPS validation. The forking approach has the sole advantage of listing the vendor of the forked module in the CMVP database. In contrast, the verification approach (what Tetrate does for Tetrate Istio Distro) offers the **smallest possible footprint of sensitive code** that must be FIPS validated and avoids the inevitable risk that a fork will drift from the more well-maintained upstream version of the module.

Applicability of validated modules. Currently validated modules under FIPS 140-2 are acceptable for use in new systems until Sept. 21, 2026, after which they will be placed on the "Historical" list. At that point, their use will be allowed only for existing systems. Agencies should continue to use FIPS 140-2 validated modules until a FIPS 140-3 validated module becomes available.

FIPS certification. *Certification* is an industry term used to apply more generally to programs like CMVP that seek to provide some kind of provable compliance with a standard. In the context of FIPS 140, *certified* essentially means *validated*.

Tetrate Istio Distro (TID) and FIPS Validation

Tetrate Istio Distro is Tetrate's hardened, performant, and fully upstream Istio distribution. It is also the first distribution of Istio to be FIPS verified for use in FedRAMP environments.

The Istio and Envoy binaries published by their respective project sites (istio.io and envoyproxy.io) are not built using FIPS-validated crypto libraries. Those binaries are not approved for use by federal authorization programs such as FedRAMP.

Tetrate solves this problem by offering Istio and Envoy binaries that are built with FIPS-validated crypto modules and independently verified by an accredited third-party testing laboratory.

Boring Crypto. Istio—and its data plane of Envoy proxies—use BoringSSL which, in turn, uses a core module called Boring Crypto. Boring Crypto is FIPS 140-2 validated (Certificate #4407). Boring Crypto's FIPS 140-2 validation status will be active until Sept. 21, 2026, and the Boring Crypto team is actively working towards FIPS 140-3 validation.

Tetrate Istio Distro FIPS builds. When pursuing FIPS validation for Istio and Envoy in TID, we used an existing crypto module that has already been validated (BoringSSL's Boring Crypto). We then engaged an NVLAP-accredited testing lab to verify that our distribution uses the CMVP-validated crypto module correctly. This lets us deliver **100% upstream Istio and Envoy** in TID, with no need for proprietary forks. And, when Boring Crypto achieves FIPS 140-3, we will update TID FIPS build certification accordingly.

A less desirable option would have been to fork a crypto library, independently maintain it, and get it validated and listed in the CMVP database, then validate that the resulting distribution uses the CMVP validated crypto module correctly.

Although our approach to getting FIPS validation for Istio and Envoy means Tetrate and TID do not have a unique entry in the CMVP database, we believe it is obviously better for users of TID and the Istio and Envoy communities since it does not require forking the highly sensitive functionality in cryptographic libraries.

Tetrate Istio Distro Is the Fastest Way to Get to Production with Istio

When you want to deploy Istio in production, the first question is where to get your Istio distribution. Tetrate Istio Distro is Tetrate's hardened, performant, and fully upstream Istio distribution. Teams often choose to run TID because it's simple to use and is built and supported by Tetrate's Istio experts (in addition to being co-creators of Istio, we also built the official CNCF course on Istio).

TID support and FIPS validated builds are available as a paid subscription service, Tetrate Istio Subscription. It's a great way to get started with Istio knowing you have a trusted distribution to begin with, have an expert team supporting you, and also have the option to get to FIPS compliance quickly if you need to.

About Tetrate

Rooted in open source, Tetrate was founded to solve the application networking and security challenges created by modern computing so enterprises can innovate with speed and safety in hybrid and multi-cloud environments. As applications evolve into collections of decentralized microservices, monitoring and managing the network communications and security among those myriad services becomes challenging. This is why some of the largest financial institutions, governments and other enterprises rely on Tetrate to deliver modern application networking and security on a foundation of Zero Trust.

Find out more at www.tetrate.io.

Tetrate Academy

If you are new to service mesh and Kubernetes security, we offer free online courses at Tetrate Academy that will quickly get you up and running with Istio and Envoy. Our courses are expertly curated, hands-on training experiences from the co-creators of open source Istio and Envoy. Private training for enterprise customers available upon request.

Learn more at academy.tetrate.io

Get Started with TIS

If you're looking for a fast way to get to production with Istio, check out Tetrate Istio Distribution (TID), Tetrate's hardened, fully upstream Istio distribution, with FIPS-verified builds and support available. It's a great way to get started with Istio knowing you have a trusted distribution to begin with, an expert team supporting you, and also have the option to get to FIPS compliance quickly if you need to.

Get Started with TSB

As you add more apps to the mesh, you'll need a unified way to manage those deployments and to coordinate the mandates of the different teams involved. That's where Tetrate Service Bridge comes in. Learn more about how Tetrate Service Bridge makes service mesh more secure, manageable, and resilient here, or contact us for a quick demo

Additional Resources

For more information about the service mesh and Tetrate's solutions, visit https://tetrate.io/resources/