EVERTRUST

Use case: TLS Server Certificates

Transport Layer Security (TLS) is crucial for securing online communications. Used in web browsing, email, and VoIP, TLS ensures privacy, integrity, and authenticity through cryptographic techniques and digital certificates.

This use case explores TLS's functionality, its evolution from SSL, and its vital role in modern cybersecurity.

Introduction to TLS Server Certificates

In today's digitized world, the security of communications over the Internet is paramount. Whether browsing websites, sending emails or making voice calls, the need for confidentiality, integrity and authenticity in data exchange cannot be overemphasized

Transport Layer Security (TLS) is the key protocol that ensures that our online interactions remain private and secure. This article explores the essentials of TLS, its applications and its evolution from Secure Sockets Layer (SSL).

Transport Layer Security: Ensuring Secure Communications

Transport Layer Security (TLS) is a cryptographic protocol designed to secure communications over computer networks.

Widely used in email, instant messaging, voice over IP (VoIP), and most notably in securing HTTPS traffic, TLS ensures privacy, data integrity, and authenticity through cryptographic techniques and digital certificates.

Developed from the obsolete Secure Sockets Layer (SSL), TLS was first defined by the Internet Engineering Task Force (IETF) in 1999, with the latest version, TLS 1.3, established in 2018.

Client-server applications use TLS to prevent eavesdropping and tampering and typically, port 443 is used for encrypted HTTPS traffic but as an alternative, a STARTTLS request can switch a connection to TLS in protocols such as email.

The TLS handshake involves

1. Cipher Suite Selection: The client and server agree on encryption and hash functions.

2. Certificate Exchange: The server provides a digital certificate for authentication.

3. Key Exchange: A secure method generates a session-specific key for encryption.

This process ensures the privacy, authenticity and integrity of the connection.
TLS supports multiple cryptographic algorithms, and its continuous updates respond to emerging security threats, keeping online communications secure.

In short, TLS is vital to protecting online interactions, providing a robust framework for secure data exchange and adapting to evolving cybersecurity challenges.

Use case: TLS Server Certificates

EVERTRUST

Importance of SSL Certificates

SSL certificates play a key role in the TLS protocol by providing encryption, authentication and assurance of accuracy and reliability of information in secure communications:

-Encryption: SSL certificates enable the encryption of the data transmitted between a web server and a user's browser, safeguarding sensitive information during transmission.

This encryption prevents unauthorized parties from intercepting and interpreting the data, protecting it from risks such as hacking and data breaches.

-Authentication: SSL certificates authenticate the identity of a Web site, ensuring that visitors are connecting to the legitimate server and not a malicious imposter.

This authentication builds consumer confidence by confirming that they are interacting with a secure and credible Web site.

-Integrity: SSL certificates ensure data integrity by using cryptographic techniques to verify that data remains intact and unaltered during transit.

This prevents malicious actors from tampering with the data, maintaining its accuracy and reliability.

Together, TLS and SSL certificates form the backbone and the perfect team for secure online communications,

Key players involved in TLS

Include a range of personas and organizations, each with specific roles:

CISO

They implement TLS to protect sensitive data, ensure regulatory compliance and manage security risks by ensuring that communications and data exchanges are protected.

CERTIFICATION AUTHORITIES

They validate the entities that request certificates, issue SSL/TLS certificates and ensure the integrity and security of their certificate issuance processes.

CA/ BROWSER FORUM

Develop guidelines for the issuance and management of digital certificates establishing standards for SSL/TLS certificates ensuring the security of Internet communications and maintaining trust in digital certificates.

SOFTWARE PROVIDERS

Develop and maintain PKI-enabled browsers and other applications, implement TLS support in their software, following CA/Browser Forum guidelines, and ensure that their software correctly handles certificate validation and encryption

INDUSTRY STANDARS

Provide accreditation and audits for CAs and other entities to ensure compliance with established security standards.

SERVER ADMINISTRATORS

Manage and maintain the organization's servers, (installation and configuration of SSL/ TLS) ensuring encrypted and authenticated communications.

Implementation and Maintenance of TLS

Steps Involved:

1. **Certificate Management**: Server administrators obtain SSL/TLS certificates from trusted Certificate Authorities (CAs). These certificates are then installed on servers to enable encrypted communications.

2. **Configuration**: Proper configuration of TLS settings is essential. This includes selecting strong cipher suites, enabling protocols, and configuring certificate chains.

3. **Monitoring and Updating**: Continuous monitoring of TLS configurations and regular updates are necessary to address emerging security vulnerabilities and ensure compliance with industry standards.

Benefits of Using TLS:

- **Enhanced Security**: TLS encrypts data, providing a secure channel for communication and protecting against various cyber threats.

- **Trust and Reputation**: Organizations using TLS can build trust with their customers and partners, demonstrating a commitment to security.

- **Regulatory Compliance**: Implementing TLS helps organizations meet regulatory requirements, avoiding potential fines and legal issues.

The reasons why TLS is important

TLS is really important for theses four major points :

DATA PROTECTION

Encrypts data transmitted over the Internet, protecting it from interception, tampering and forgery maintaining user privacy and protecting sensitive information.

TRUST AND AUTHENTICATION

It uses certificates issued by (CA) to authenticate the identity of websites, helping users to verify that they are connecting to legitimate sites.

COMPLIANCE AND STANDARDS

Regulations and standards, such as GDPR and PCI DSS, recommend or require the use of TLS to protect data in transit.

ATTACK PREVENTION

Prevent various attacks, including man-in-the-middle attacks and data breaches, improving overall cybersecurity.

Challenges in TLS Management

Challenge	Details	How EVERTRUST address it
1. Certificate Lifespan and Management	The complexities of managing TLS certificates, especially with Google's reduced certificate lifespans, increase the frequency of renewals and the administrative burden.	EVERTRUST efficiently manages certificate assets across both local and cloud environments, simplifying this process and reducing errors.
2. Automation and Scalability	Need for automation to handle frequent renewals.	EVERTRUST provides seamless integration of automated certificate management, facilitating scalability. This aligns with Google's promotion of ACME services, ensuring that even with increased renewal frequency, systems remain manageable and efficient.
3. Infrastructure Modernization	Modernizing infrastructure to adapt to new standards, like limiting root CA certificates and phasing out multipurpose roots, requires significant changes.	EVERTRUST supports this by enabling smooth transitions from on-premises to cloud environments without major reconfigurations, helping organizations meet modernization demands with minimal disruption.
4. Accountability and Compliance	Ensuring compliance with new policies, such as mandatory audits for non-TLS subordinate CAs, requires continuous oversight.	EVERTRUST helps maintain up-to-date practices by providing robust eIDAS-compliant management tools ensuring compatibility and compliance and automates processes using security protocols with a streamlined approach improving efficiency and accuracy, minimizing disruptions and maximizing integration into existing IT systems.
5. Preventing Outages	Disrupting services and compromising security through certificate expiration,	EVERTRUST improves application performance and reliability by managing the discovery, issuance, deployment, renewal and revocation of certificates, mitigating the risks of disruptions by ensuring the smooth renewal of certificates and the availability of CRLs and OCSP responses. All while maintaining control over cryptographic keys.

Use case: TLS Server Certificates

EVERTRUST

Conclusion

After all, transport layer security (TLS) is vital to securing online communications, safeguarding data and maintaining user trust. Automating certificate management-including discovery, deployment, lifecycle management and renewal-transforms this traditionally manual and error-prone task into a streamlined and strategic process.

This automation not only mitigates risk, but also improves security and operational efficiency, ensuring that organizations are well prepared for future challenges. Effective TLS management, while crucial, involves overcoming obstacles related to certificate lifecycle, automation, infrastructure upgrades and regulatory compliance.

By implementing comprehensive, automated certificate management solutions, organizations can significantly improve their security posture, minimize manual errors and ensure continuous, secure operations in an ever-evolving security landscape. And as we've explained above, EVERTRUST’s tools make all this possible and more!

GET RID OF CERTIFICATE OUTAGES AND REDUCE PKI OPERATING COST WITH EVERTRUST

Use case: TLS Server Certificates

WE CREATE...

- Operational, secure and high-performance solutions that articulate IT security and control the lifecycle of electronic certificates.
- Integrated in a non-intrusive, simple and effective way into our customers' existing ecosystems.
- Designed to meet the needs of trusted service delivery, automation and continuity.

Stream

- ✓ Hold your own Keys without Captivity
- ✓ Issuance and revocation of certificates
- ✓ Issuance of CRLs, OCSP responses and timestamping
- ✓ eIDAS ready and compliant
- ✓ Designed to be deployed on premises or in the cloud

Horizon

- ✓ Streamlined integration within the information system
- ✓ Process certificate lifecycle requests using comprehensive workflows and machine identity management tools
- ✓ Take care of the issuance, renewal, and revocation of certificates hosted on:
  - Servers, mobiles and workstations
  - Appliances and IoT
  - On premises or in the Cloud

EVERTRUST

EVERTRUST

Use case: TLS Server Certificates

Discover more !

evertrust.io

Use case: TLS Server Certificates