Secure Data Transport for Networks and Endpoints

Eclipz secure data transport embeds in networks and endpoints to secure data in transit over public or private P2P / multipeer communications

Version 3

Eclipz.io, Inc.
20 S. Santa Cruz Ave., Suite 300
Los Gatos, CA 95030
https://eclipz.io

TABLE OF CONTENTS

Making secure data transport easy and transparent

Peer-to-peer and multipeer communications must be secure to safely exchange all sensitive data, including applications, financial data, messages, and numerous proprietary documents and records. Communications should be authenticated and authorized based upon policy and then secured from end to end, with no passthrough hub intercepting unencrypted data, and traffic must be encrypted throughout the network so adversaries cannot hijack the communications. Ideally, communications are secured automatically to eliminate the dependency on ordinary end users to operate complex security protocols. End users shouldn't be empowered (or for that matter, burdened) to determine what data they should or should not protect and which security protocol to follow. To date, most secure transactions involve a weighty burden on both users and vendors:

- Users need to understand appropriate encryption methods for the data they are securing, follow corporate security protocol, and use special software or devices.
- Vendors need to provide custom devices and configuration and elaborate infrastructure.

Secure communications have therefore been more of a dream than a reality in the commercial world, limited to constrained, controlled, and expensive environments.

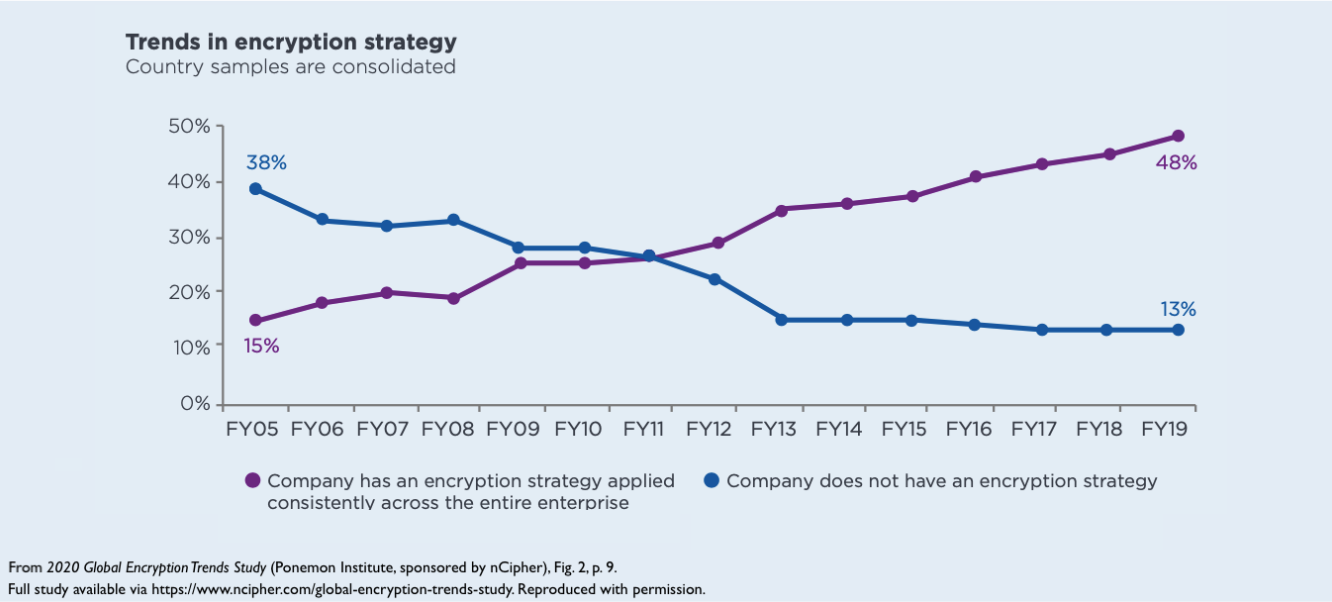
This whitepaper explores how Eclipz's secure data transport removes the challenges that enterprises face when attempting to authenticate then determine from policy the authorization to both connect and apply the appropriate crypto to secure data as it moves between the sending and receiving endpoints. We'll look at enclaves, private key management systems, and practices with regards to the risk and complexity they pose to the network, administrators, and end users.

Encryption grows while key management problems persist

The *2020 Global Encryption Trends Study* (Ponemon Institute, sponsored by nCipher) documented a dramatic increase in companies with an enterprise-wide encryption strategy, growing from 15% in 2005 to 48% in FY2019.[1] The most substantial security risk cited was employee mistakes, followed by system malfunctions, then hackers. The greatest barriers to planning and executing an enterprise data encryption strategy include identifying where the sensitive data resides and in classifying it, the initial deployment process, and the ongoing management of the encryption and keys. Training users to correctly use encryption is also a concern.[2]

[1] *2020 Global Encryption Trends Study* (Ponemon Institute, sponsored by nCipher), p. 9. Retrieved November 03, 2020, from https://www.ncipher.com/global-encryption-trends-study

[2] Ibid., p. 12.



From *2020 Global Encryption Trends Study* (Ponemon Institute, sponsored by nCipher), Fig. 2, p. 9.
Full study available via https://www.ncipher.com/global-encryption-trends-study. Reproduced with permission.

With employee mistakes and system malfunctions being entirely within a company's control, yet apparently uncontrollable, it's clear that a successful protection strategy cannot depend on users and systems behaving correctly.

The 6,457 study respondents said their primary reasons for adopting encryption strategies were protection of customers' personal information (54%), security of intellectual property (52%), and protection against specific, identified threats (51%).[3]

To enable an enterprise encryption strategy, data requires protection for several critical activities:

- Internet communications
- Transmission within the enterprise and to trusted partners and vendors
- Transmission to the cloud, and on occasion, when changing cloud providers
- Financial transactions to and from customers
- Passing any personal, proprietary, private, identifiable, or other regulated data over a network

Companies encrypt their data before sending it to the cloud (45%), trust the cloud provider (and the network during transmission to the cloud) to provide encryption (36%), or encrypt in the cloud using and managing their own keys on-premises (20%).[4] Encryption trends have shifted over the years, as companies first concluded that the cloud was secure, and then increasingly realized that shared cloud environments are not inherently as secure as desired and that even if the cloud is secure, moving data to or from that cloud increasingly requires encryption in transit.

Secured and encrypted data includes databases, Internet communications, data center storage, internal networks, employee computers (including mobile laptops and phones), and hosted applications like email. Collectively these represent a wide variety of storage formats, devices, and transport

[3] Ibid., p. 5.

[4] Ibid., p. 24.

methods; not surprisingly, key management is cited as the most significant pain point, with 60% of the Ponemon Institute respondents rating the difficulty of key management as 7 or greater on a 10-point scale.[5]

Key management remains the hardest challenge for many companies deploying an encryption strategy, even for those who are only attempting an application-specific security initiative (such as email). Complex keys are sometimes stored in spreadsheets, rather than in key management systems, leaving them susceptible to mistakes due to the manual process that the administrators must employ. In fact, the 2020 Ponemon Institute study showed that 34% of the responding companies still used manual processes (spreadsheets or paper) to manage their keys.[6] Keys come with inherent problems because they're complex and hard to deploy. Key revocation is also tricky because keys expire, need to be replaced, and are hard to manage. As a result, users often get frustrated. They frequently bypass corporate security policies and requirements for using secure applications. Instead, they send information outside of the network to avoid these cumbersome keys or passphrases.

An effective strategy must protect all the critical types of data from both deliberate attack and internal mistake, reduce the burden on the administration, and it must do so in a way that does not depend on thousands or millions of users following policy.

Use your existing devices and infrastructure

Eclipz is a proven software-based peer-to-peer / multipeer communication solution for first authenticating the originating endpoint and then authorizing the connection to the destination endpoint to establish a secure, on-demand network (or enclave). Its policy determines the type of encryption (AES-128, AES-128, or future quantum) for any type of data in motion: voice, email, documents, video, text, financial transactions and more. At a high level, Eclipz mitigates the risk and complexities associated with securing data in motion over private and public networks. Eclipz is distributed to the market as an embeddable OEM plugin or a lightweight overlay for RTOS, Linux, Windows, Android, and Apple iOS. Eclipz operates on Layer 2 / 3 of the OSI model and therefore is compatible with existing network stacks, applications, endpoint systems, and mobile devices as-is—no need to rewrite or recode. Simply apply Eclipz as either an API call, or most often, as a simple configuration change to application settings. In supporting e-commerce apps for consumers, simply incorporate Eclipz into your application and have zero touch with the end-user device through app stores' downloads or other commercial distributions to a device.

The software has been deployed within the most hostile environments around the world where human lives depend on Eclipz's zero-failure reliability. Enterprises manage it; users don't have to interact with it so they can't accidentally expose or disable it; it's invisible, so attackers don't see it or any data that it's transmitting.

[5] Ibid., p. 16.

[6] Ibid., p. 18.

Eclipz's secure data transport overview

To accomplish a secure peer-to-peer or multipeer on-demand network, also called a virtual trusted network (VTN), the following must happen:

1. Validate an endpoint as a member of the network, and then direct the traffic to further determine trust.
2. Establish the authenticity and validity of the Eclipz software on the endpoint.
3. Produce on the endpoint an ephemeral certificate that is unique to the on-demand network enclave policy to which it is associated for the VTN / IPsec tunnel session.

In short, the endpoints need to be identifiable, validated, trusted, and produce their X.509 ephemeral key for each endpoint connection generation.

The first step is to **determine if an endpoint is an active member of the network** over which it is trying to communicate. An endpoint can reside anywhere or be anything. When an endpoint becomes a member of the network, Eclipz gives it a unique identity that it can validate as a trusted endpoint. When called upon, the member endpoint will uniquely identify itself to a specific location on the network that only responds to other validated member endpoints on the network. Eclipz does this by using a process referred to as dark networking. Dark networking not only reduces the attack surface of the Eclipz platform, but also prevents DDOS attacks to the system.

Once Eclipz validates an endpoint as a member of the network, the dark network entry point redirects the traffic to a specific IP address with the necessary ports and services to proceed with the next step of determining trust.

In this next step, Eclipz uses a confirmation method to **establish a *trusted validation* of the Eclipz software on the endpoint**; this validation ensures that the Eclipz software exists in its original form and has not been modified in any way. This trust mechanism is made up of several elements within the endpoint that are then *hashed* along with a *proof of work* and published to a public or private blockchain. It can include a trusted platform module (TPM) if present. This element that Eclipz publishes is used for validation when an endpoint is requested for communication. The policy sets the timing. The platform can do a lookup each connection or once a month.

Once the platform determines the endpoint is a valid member on the network, has the appropriate software installed, and is original without modification **Eclipz generates on the endpoint agent an *ephemeral certificate, using a public / private key pair generated on the endpoint agent at installation,*** which is unique to its associated enclave policy.

X.509 ephemeral (short-lived) certificates are derived much like a traditional PKI certificate, whereby they are a child relationship with a chain to the root certificate authority. However, ephemeral certificates are automated, live for a very brief period, and tie back to the Eclipz enclave policy associated with the endpoint.

Eclipz can achieve null encryption, which is an important capability option for the enclave session. Null encryption still validates endpoints and enforces policy restrictions for connections both to and from the endpoints before enabling connections. This distinction can be important for securing a mobile

workforce, or simply to lock down internal servers with microsegmentation from non-approved and validated connections without encryption. Null encryption introduces a minimal overhead to sessions since it doesn't introduce any encryption for transmissions between the authorized and validated endpoints.

Unique aspects of ephemeral certificates

An endpoint application does not even know this is happening; in many cases, it could have different certificates for every communication, considerably reducing the attack surface.

The X.509 certificates are tied to an enclave policy, which identifies which endpoints can communicate, the type of crypto to be used (AES-128, AES-256, null, or quantum), and other factors like routing or service-level agreement (SLA). Eclipz sets up an on-demand VTN transport between the devices that are dynamically adjusted to policy and specific to the communication. The VTN verifies authenticity and authorization of Eclipz-enabled clients to talk to each other upon connection request.

Managers of certificates can now focus on the higher-level certificates, root, and sub-root level, and if necessary, can change that level more often without affecting the certificates at the lower levels because they are dynamic. This considerably reduces the burden of certificate management.

> *Note: Eclipz is capable of hooking to existing certificate management systems, e.g., mid-tier and smaller organizations might use Active Directory to host their certificate authority while telecommunication companies may employ a system of systems that also tie to their policy management and billing systems.*

The steps and processes we just reviewed happen quickly and prep the network for Eclipz to conduct the dark network secure data communication. We have a trusted endpoint with a valid short-lived certificate. We now need to look up its enclave policy for this specific communication instance or on-demand VTN request.

Each endpoint is associated with at least one enclave group policy but could participate in multiple enclave groups. The enclave policy affects several aspects of what can be transported over the Eclipz secure, on-demand enclave once it is established, using this particular ephemeral certificate at this particular time. Policy configurations include the following:

- Applications that are allowed to communicate
- Ports and services available for use
- Routing requirements
- What type of encryption (AES-128, AES-256, null, quantum)
- With whom or what the endpoint can communicate

There are many other aspects of the policy that can be set, but the aforementioned list items are the essential elements of the policy. That means the policy must also be validated when a request is made for a secure communication connection.

Note: Policy management can be done directly inside the Eclipz policy manager, or can be hooked to existing policy managers, e.g., a directory service, which can inherit its policy and tie it to the secure network communications.

An example of a dark network secure communication

Endpoint A is a mobile device, and the user wants to request communication with Endpoint B, which is also a mobile device. Endpoint B is using Endpoint C, which is a service hosted by a provider such as a Session Initiation Protocol (SIP) server.

All endpoints (A, B, and C) must be registered with the Eclipz platform and in an online state. Endpoint A makes a request, which initiates the dark network enclave communication and Eclipz platform then looks up each endpoint policy. Once Endpoints A, B and C are validated, the Eclipz platform assigns a route with only the network services specified in the policy. The specific encryption determined by policy (IPsec, in most cases) to all endpoints creates a multiparty encrypted on-demand VTN among the three endpoints. The Eclipz platform then steps out of the way so that traffic is only routed between the trusted endpoints. Once the dark network communication session ends, all routing, policies, and networking vanishes, as if it never existed.

Edge / MEC

Eclipz can address the point-to-point encryption capability that secures communications between containers within a mobile edge computing (MEC) platform. Eclipz can help organizations mitigate risk of cross-contamination or attack within a shared environment, such as MEC, by encrypting container-to-container communications for any Kubernetes / containerized application with only one minor change to the Kubernetes environment to make this possible.

Eclipz software can be used to enable MEC outposts in providing the encryption services that isolate an enterprise's applications and data through container-to-container enclaves. The Eclipz-enabled MEC will also ensure users' and machines' communication are protected, and network overhead and latency are minimized. Eclipz is a foundation to create the confidence users and enterprises require to realize the promise of 5G and MEC.

SASE

Enterprise networks are being called upon to handle more external traffic than ever before, as traffic travels to and from cloud and SaaS environments, IoT devices, mobile users, and remote workers. Each endpoint needs connectivity into the network, and enterprises must secure those connections and any resulting traffic. Having to backhaul the traffic to the data center to undergo security inspection impedes efficiency and user experience.

With Secure Access Service Edge (SASE), enterprises can distribute networking and security services—such as URL filtering, DNS, software-defined WAN (SD-WAN), and secure web gateway—directly to any endpoint, regardless of where it connects to the network, according to Gartner.

Eclipz brings a significant enablement to the SASE capability. It changes the economics and utility of network layer / IPsec encryption, enabling a standard approach to encryption, and can be embedded into the SASE fabric to secure data in transit across SASE offerings.

Visibility is not constrained by application towers but allows unified experiences across SASE offerings. Eclipz provides the isolation and access to edge-based resources while reducing complexity and latency of routing and adjusting for SLAs by the enclaves, which allows for the monitoring and inspecting of encrypted and null-encrypted data in motion.

One key capability required for SASE is an agent for the endpoints. The Eclipz agent enhances a SASE agent by:

- Enabling issuance of identity- and role-based credentials.
- Monitoring and enforcement of multi-factor trust and risk assessments.
- Anchoring of the agent to the TPM.

Eclipz optimizes connections to data loss protection (DLP), malware inspection, and behavior analytics through APIs and SDKs while protecting traffic over untrusted networks.

Conclusion

Corporate security is cumbersome. Enterprises rely on end users to always abide by corporate security policy. While users are expected to maintain these security standards, and to some degree understand concepts such as certificates and security best practices, it’s unrealistic to think that they will. The advancement of mobile communication and productivity devices has made us a much more transient society. We work at home, in airports, restaurants, and just about anywhere we find ourselves during the week. Peer-to-peer and multipeer telecommunications must be secure to safely exchange sensitive corporate communications and information. Because most corporate workers aren’t security experts and need to focus on their job functions, it’s critical to implement security solutions and initiatives that not only mask the complexity of securing data transmissions, but also enforce security policy no matter what the user chooses to do—or not to do—relative to enterprise security protocol.

Eclipz is a proven secure data transport-embedding technology. It’s been in deployment by the US Government since 2015, securing data communications around the world. Eclipz automates secure data communications, so it's easy for enterprise security teams to manage and transparent to end users. Partners that embed Eclipz can offer their customers solutions that ensure corporate data and communications are secure from attack 24 hours a day, 7 days a week, 365 days a year.