WHITEPAPER

Email Encryption securing digital communication

Use case: Email Encryption

EVERTRUST

Introduction to Email Encryption

Emails have become a prevalent method for online communication, serving various purposes such as corporate correspondence or personal interactions.

To standardize the transmission and reception of emails, open protocols like IMAP, SMTP, and Exchange were devised and implemented.

However, these protocols lack inherent security measures, notably mechanisms for recipient verification of sender identity (absence of authentication and non-repudiation), that consequently exposes less tech-savvy employees within organizations to potential phishing attacks.

Use case: TLS Server Certificates

EVERTRUST

But first, let’s understand: What is E-mail Encryption?

Email encryption converts readable text into an encoded format that can only be decrypted by someone with the correct key.

There are two main types of email encryption: symmetric and asymmetric.

Here, we will focus on the most common: asymmetric encryption, which uses a key pair:

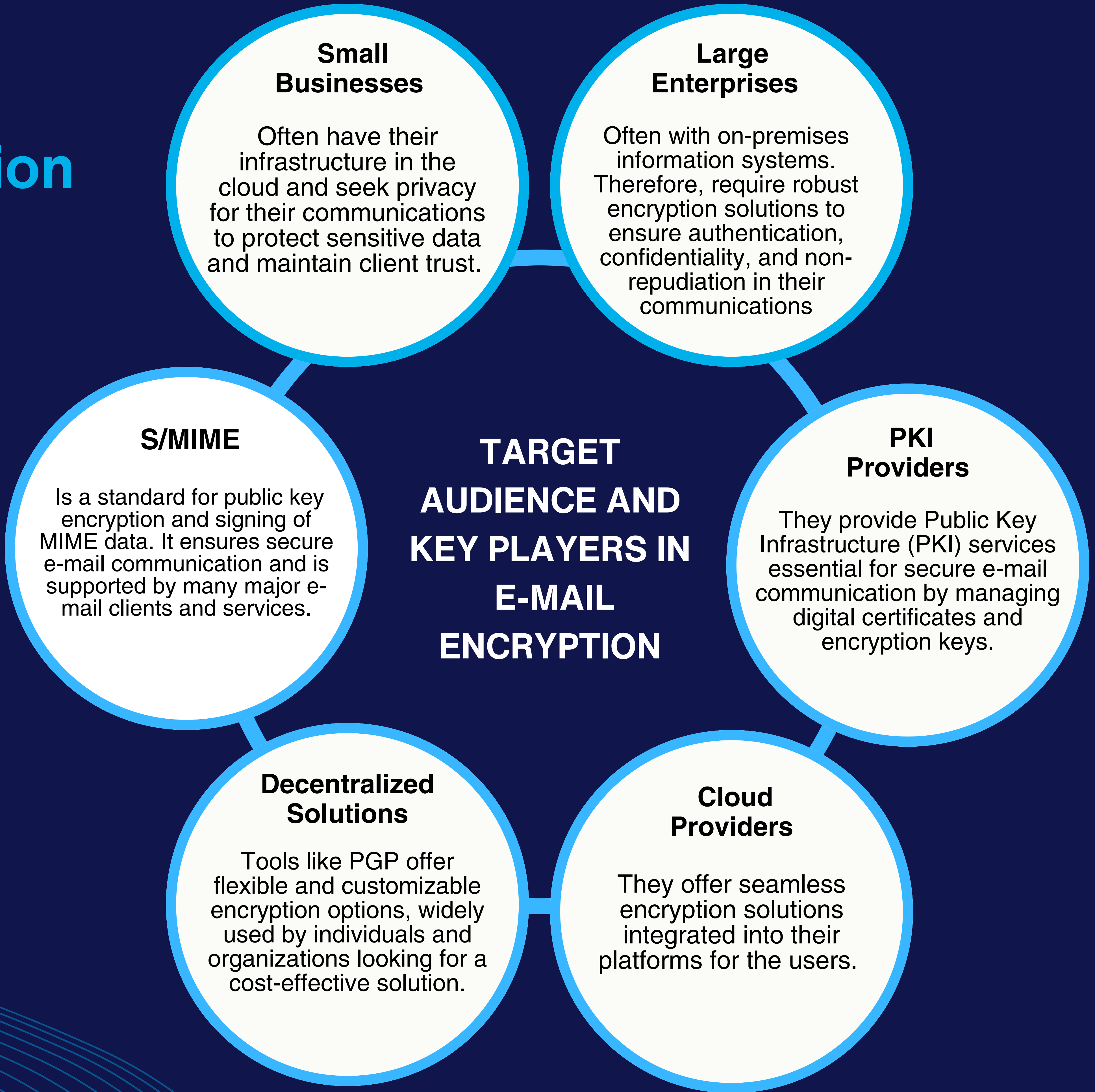
- A public key for encryption.
- A private key for decryption.

This method offers higher security, since the private key is never shared.

Target audience and key players in E-mail Encryption

E-mail encryption is crucial for a wide range of users, encompassing both small businesses and large enterprises, each with distinct needs for privacy, authentication, confidentiality, and non-repudiation. The target audience for e-mail encryption includes all the following graph.

By leveraging these players and solutions, users can effectively secure their e-mail communications against unauthorized access and threats.



TARGET AUDIENCE AND KEY PLAYERS IN E-MAIL ENCRYPTION

Small Businesses

Often have their infrastructure in the cloud and seek privacy for their communications to protect sensitive data and maintain client trust.

Large Enterprises

Often with on-premises information systems. Therefore, require robust encryption solutions to ensure authentication, confidentiality, and non-repudiation in their communications

PKI Providers

They provide Public Key Infrastructure (PKI) services essential for secure e-mail communication by managing digital certificates and encryption keys.

Cloud Providers

They offer seamless encryption solutions integrated into their platforms for the users.

Decentralized Solutions

Tools like PGP offer flexible and customizable encryption options, widely used by individuals and organizations looking for a cost-effective solution.

S/MIME

Is a standard for public key encryption and signing of MIME data. It ensures secure e-mail communication and is supported by many major e-mail clients and services.

Use case: Email Encryption

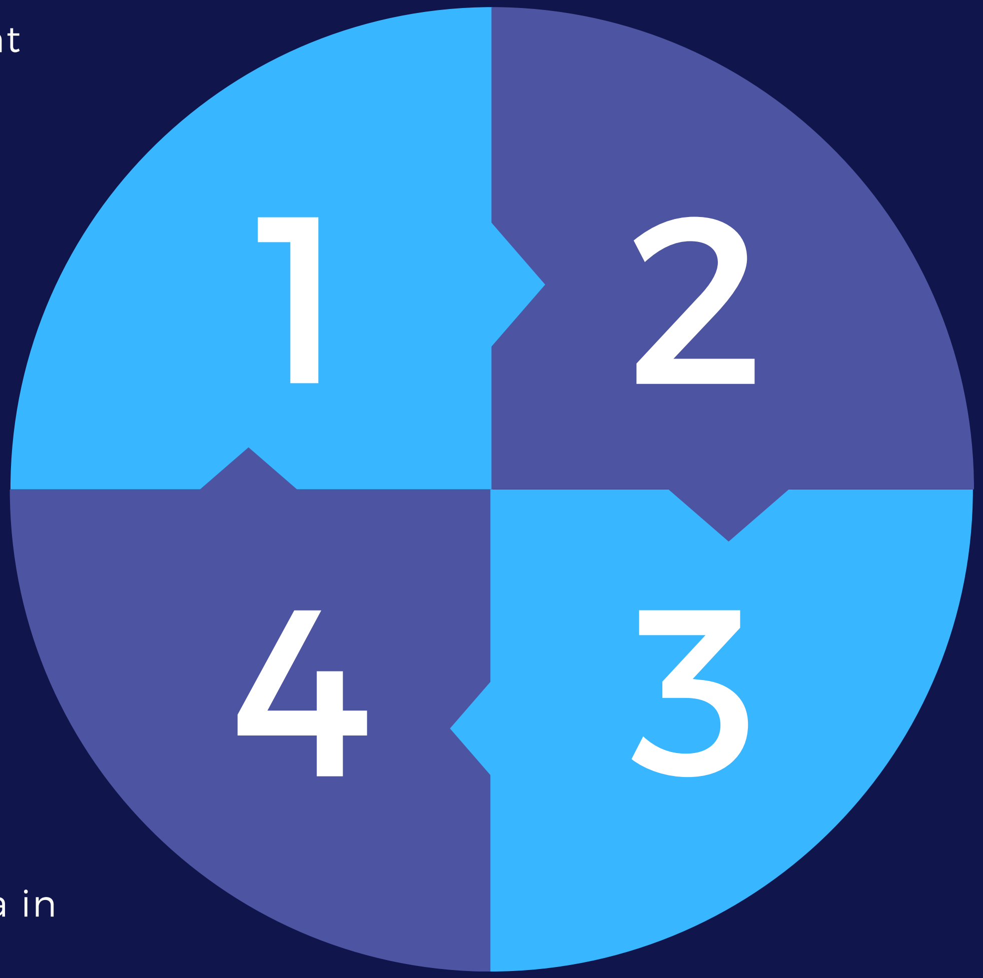
EVERTRUST

Use case: Email Encryption

Why E-mail Encryption is Essential?

Email is a primary communication tool for both personal and professional use, frequently containing sensitive information such as personal identification details, financial data, and confidential business information.

Without proper encryption, emails can be intercepted, read, and altered by malicious actors during transmission. Encryption ensures that only the intended recipient can access the content, preserving both confidentiality and integrity.



1 Confidentiality

Ensures that email content remains private and accessible only to the intended recipient by transforming email content into a format unreadable to unauthorized users.

2 Authentication

Verifies the identity of communicating parties, ensuring that emails are sent and received by legitimate users. Digital signatures used in encryption protocols help prevent spoofing and ensure reliable communication.

3 Non-repudiation

It ensures that the sender cannot deny sending an email and the recipient cannot deny receiving it. Digital signatures and encryption provide proof of origin and receipt, which is crucial for accountability in legal and business contexts.

4 Cloud Adoption & Eavesdropping Concerns

The shift to cloud services for email hosting has increased the need for encryption to protect data in cloud environments. In addition, the threat of eavesdropping, where unauthorized persons intercept emails during transmission,

EVERTRUST

Some popular email encryption protocols:

PGP/GPG

PGP (Pretty Good Privacy) and GPG (GNU Privacy Guard) are widely used encryption protocols that rely on symmetric encryption, using the same key to encrypt and decrypt data. Both the sender and the recipient(s) must have the key. PGP can only encrypt the text body of emails, leaving attachments unencrypted. Additionally, PGP only provides encryption and does not offer authentication and non-repudiation.

Google Client-Side Encryption

This solution provides email encryption and signature without the need to manage a PKI. Since it heavily relies on S/MIME, it will not be further detailed here.

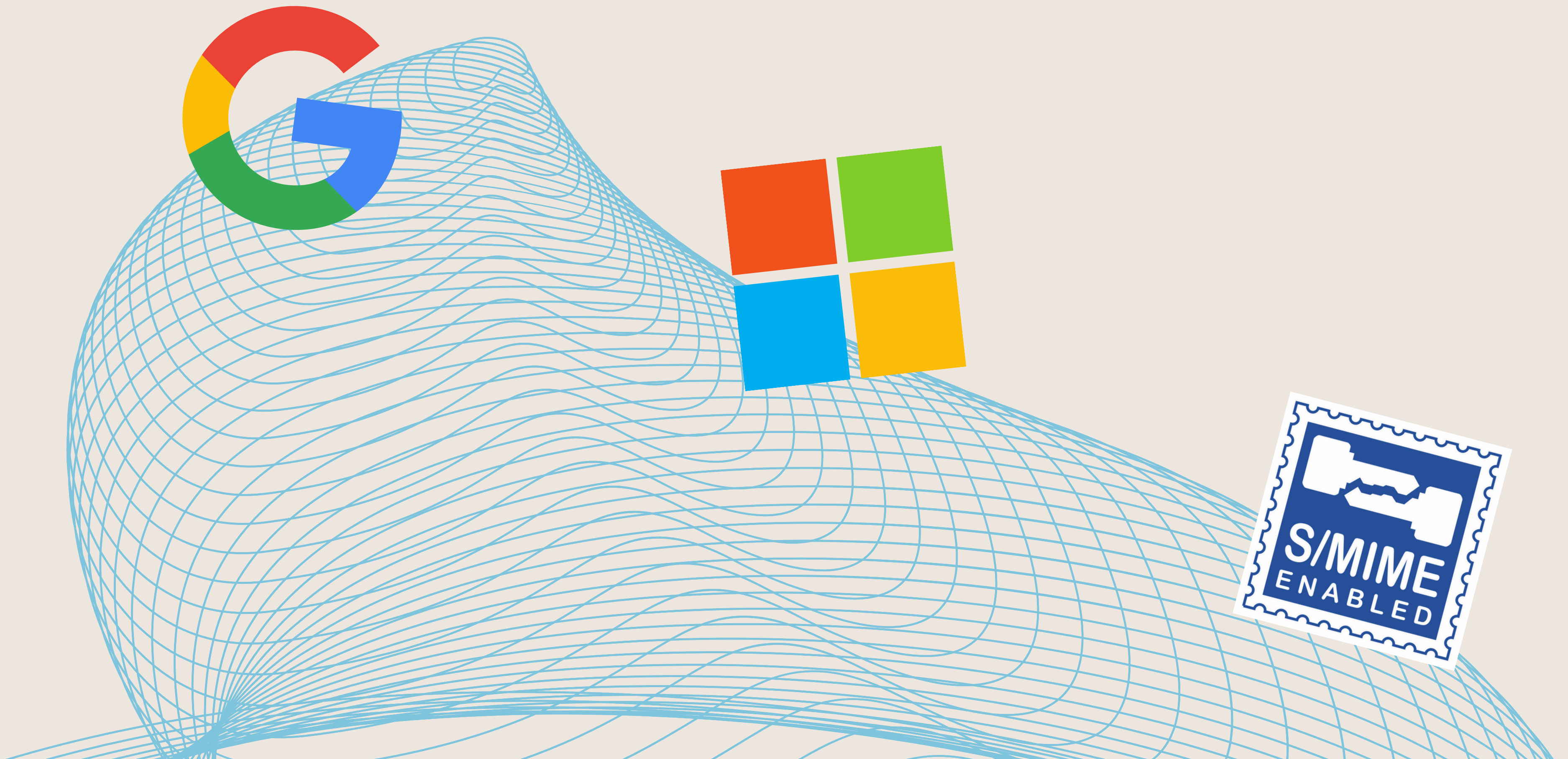
Considering the increasing prevalence of cyber threats, staying informed and proactive about email encryption is essential for maintaining secure digital communication.

Microsoft 365 Message Encryption

This solution is applicable only to Outlook for Office 365 with an Enterprise license. Microsoft provides a way to send emails with an access control system like what's available on the rest of the Azure platform. However, this requires the sender to use Office and does not apply to other email services.

S/MIME

S/MIME (Secure/Multipurpose Internet Mail Extensions) relies on certificates and PKI (Public Key Infrastructure) to provide encryption and signature for emails, granting confidentiality, authentication, and non-repudiation. Encrypted messages in S/MIME are CMS blobs (PKCS#7 format) and can only be decrypted with the private key used to encrypt them. The PKI environment ensures that a certificate is trustworthy, as it is issued by a trusted certificate authority.



Implementing S/MIME with EVERTRUST Stream

Benefits of EVERTRUST Stream:

- Management of multiple CAs and certificate templates.
- Support for RSA, elliptic, and Edwards curve keys.
- Integration with cloud key management solutions and HSMs .

EVERTRUST Stream is essential for addressing these issues as it functions as a certificate authority. It serves as the foundation of a Public Key Infrastructure (PKI) by enrolling signature and encryption certificates that can be utilized through S/MIME or Google Client Side Encryption.

EVERTRUST Stream manages multiple certificate authorities (CAs) and certificate templates simultaneously, making it ideal for environments where certificate usage is highly segregated, necessitating the issuance of signature and encryption certificates from different CAs.

Additionally, EVERTRUST Stream supports signing with RSA keys (up to 8192 bits), elliptic curve keys, and Edwards curve keys, and it natively handles keys from Cloud Key Management Solutions (AWS KMS, Azure Key Vault, GCP CKM) or Hardware Security Modules (HSMs) via its PKCS#11 interface.

Implementing S/MIME with EVERTRUST Horizon

EVERTRUST Horizon is the core component of the solution. It relies on an existing PKI (such as Stream) to issue certificates, delegating cryptographic operations to the PKI. Horizon supports various integrations to streamline certificate enrollment and deployment:

Central Registration Authority

- Horizon supports various key types (RSA 2048, RSA 3072, RSA 4096, elliptic curves, and Edwards curves) and offers both decentralized and centralized enrollment. In centralized enrollment, Horizon can escrow the certificate’s private key for recovery purposes, as seen in the Intune integration in PKCS mode.

Escrowed Certificates for Mobile Devices

- The SCEP protocol does not support centralized enrollment, making it impossible to escrow certificates for encryption. However, Horizon supports the PKCS mode of Intune to securely push escrowed certificates to devices without exposing the private key to Intune.

Mobile Device Integration:

- Signature certificates can be issued through the SCEP protocol, supported by most MDM servers like Intune, Jamf, Mobicontrol, MobileIron, or Workspace One. Horizon integrates seamlessly with Intune and Jamf, automatically revoking certificates when an asset is decommissioned from the MDM server.

Windows Active Directory Integration

- The WCCE protocol, combined with the WinHorizon proxy, allows auto-enrollment of required certificates (signature and encryption) on the corporate PKI. New users connecting to Active Directory for the first time automatically receive their user certificates without manual intervention.

Certificate Publication

- Horizon can publish all enrolled certificates in an LDAP directory, including any Microsoft Active Directory, which is crucial for encryption certificates to be used by others to encrypt data sent to the certificate holder.

Key Considerations for S/MIME Certificate Implementation

Separate Certificates for Signature and Encryption

- Ensure there are distinct certificates for signature and encryption, which may come from the same or different CAs.

Single Valid Encryption Certificate

- Only one valid encryption certificate should be in use at a time to avoid confusion in encryption processes and to ensure all recipients can decrypt the messages.

Escrowing Encryption Certificates

- Encryption certificates should be escrowed to allow recovery of the private key if lost. Retaining former encryption certificates is recommended for decrypting data encrypted with previous certificates.

By following these guidelines, the implementation of S/MIME with EVERTRUST Stream and Horizon can be efficient and secure, ensuring seamless certificate management and deployment.

Use case: TLS Server Certificates

EVERTRUST

Steps to Implement S/MIME in your company using EVERTRUST Stream and Horizon

These steps can be easily implemented using EVERTRUST products, thanks to the seamless integration between the CA (Stream) and the RA/CLM (Horizon).

The numerous automation features and various integrations ensure that each S/MIME certificate use case can be effectively addressed through Stream and Horizon.

01

Establish a Public Key Infrastructure

- Start by setting up a PKI, such as EVERTRUST Stream
- Create certificate templates specifically for signature and encryption, ensuring the correct key usages are defined.

02

Connect a Registration Authority (RA)

- Integrate a registration authority like EVERTRUST Horizon with your PKI.
- Configure the connector on the appropriate Certificate Authority (CA) and template to issue S/MIME certificates for both signature and encryption.

03

Configure Integrations

- Set up the desired integration through the supported protocols of your RA.
- With Horizon, all integrations are supported, allowing Horizon to issue certificates for various use cases and deploy them directly on the required devices.

04

Automate Certificate Renewal

- Configure the automatic renewal of certificates to ensure their lifecycle is fully automated.
- Utilize CLM system, which EVERTRUST Horizon includes. This feature enables comprehensive management of certificate lifecycles from issuance to expiration, renewal, or revocation via a unified interface.

Conclusion

Email encryption is a vital element of contemporary digital security, safeguarding sensitive information from unauthorized access and ensuring the integrity of communications.

By comprehending the various encryption methods, deploying the appropriate tools, and adhering to best practices, individuals and organizations can effectively protect their emails. As cyber threats continuously evolve, staying informed and proactive about email encryption is crucial for maintaining secure digital communication.

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: Email Encryption

Discover more !

evertrust.io

Use case: TLS Server Certificates

EVERTRUST