# REPORT
# Kerberos Authentication Protocol

*v1.0.0*

Author:

**Eldon Gabriel**

August 22, 2025

# TABLE OF CONTENTS

## REVISION HISTORY

| Version | Date | Author | Description of Changes |
|---|---|---|---|
| v1.0.0 | 08/22/2025 | Eldon G. | Initial draft. |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# EXECUTIVE SUMMARY

Kerberos is a network authentication protocol that prevents sending passwords in plain text. It uses a Key Distribution Center (KDC) to issue encrypted, time-limited tickets. This report covers the security problem Kerberos solves, the main components (client, Authentication Server, Ticket Granting Server, and services), and its use in modern environments like Single Sign-On (SSO) and Microsoft Active Directory. By combining a trusted authority, encryption, and short-lived tickets, Kerberos provides secure, scalable authentication for enterprise networks.

---

# 1.0 INTRODUCTION TO KERBEROS

## 1.1 Background: The Problem Kerberos Solves

Historically, networks were built for efficiency, not security. Before Kerberos, users had to send their usernames and passwords to each service individually. This exposes credentials to network eavesdropping and man-in-the-middle attacks. As networks expand, these vulnerabilities become critical. Kerberos was developed to provide a secure way for users and services to authenticate without exposing raw credentials.

## 1.2 How Kerberos Works

Kerberos introduces a **trusted third party**, the Key Distribution Center (KDC), which centralizes the authentication process. Instead of sending passwords, clients request encrypted, time-limited tickets from the KDC. These tickets prove identity and cannot be reused if they are intercepted.

## 1.3 Purpose: Secure and Scalable Authentication

Kerberos uses strong encryption and synchronized time stamps to prevent replay attacks. Its centralized design supports Single Sign-On (SSO), allowing users to access multiple resources after a single login. This makes Kerberos ideal for large organizations and enterprises.

---

# 2.0 CORE COMPONENTS AND TERMINOLOGY

## 2.1 The Key Distribution Center (KDC)

**Key Distribution Center (KDC):** a central authority that manages authentication. Two main functions:

1. **Authentication Server (AS):** Verifies users and issues the Ticket Granting Ticket (TGT).
2. **Ticket Granting Server (TGS):** Issues Service Tickets (ST) for specific resources after validating the TGT.

**Client:** The machine or user requesting access to the services. It interacts with the KDC to obtain tickets instead of directly sending passwords.

**Server:** Hosts resources or applications. It validates tickets before granting access to the user.

**Tickets:** Encrypted tokens that prove identity.

**Ticket Granting Ticket (TGT):** Enables clients to request multiple service tickets without having to resend their passwords.

**Service Ticket (ST):** Grants access to a specific server or application.

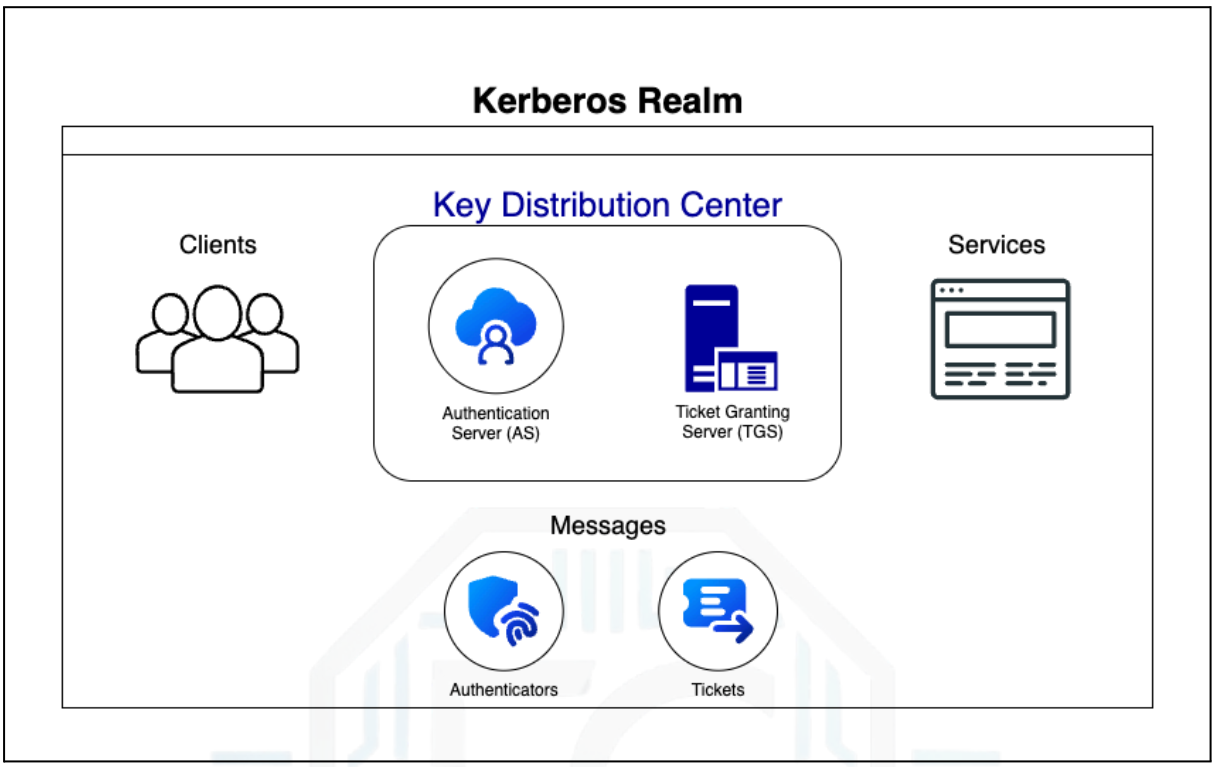


**Figure 1**: DIAGRAM - Kerberos Realm Components - v1.0.0. 2025. Eldon

# 3.0 THE KERBEROS AUTHENTICATION PROCESS

Kerberos authentication relies on the exchange of encrypted tickets instead of passwords. The lifecycle involves six steps where the Authentication Server (AS), Ticket Granting Server (TGS), and service all play distinct roles in verifying identity and granting access.

## 3.1 Step 1: Authentication Service Request (AS)

The client initiates contact with the AS to request access. The AS verifies the user's identity using credentials derived from the user's password.

## 3.2 Step 2: Ticket-Granting Ticket (TGT) Issuance

If authentication succeeds, the AS responds with a **TGT** and a **TGT session key**. The TGT is encrypted so only the TGS can read it, while the session key allows secure communication between the client and TGS.

## 3.3 Step 3: Ticket Granting Service Request (TGS)

The client uses the TGT to request a service ticket from the TGS. Along with the TGT, the client also sends an authenticator to prove it is the same entity that received the TGT.

## 3.4 Step 4: Service Ticket Issuance

The TGS validates the TGT and authenticator. Once verified, it issues a **Service Ticket (ST)** and an **ST session key**, which are used for communication with the target service.

## 3.5 Step 5: Service Request

The client presents the **ST** and a fresh authenticator to the target service. This step ensures replay protection and proves the client's identity to the service.

## 3.6 Step 6: Service Validation and Access

The service decrypts and validates the ST and authenticator. If successful, the service grants the client access to the requested resource.

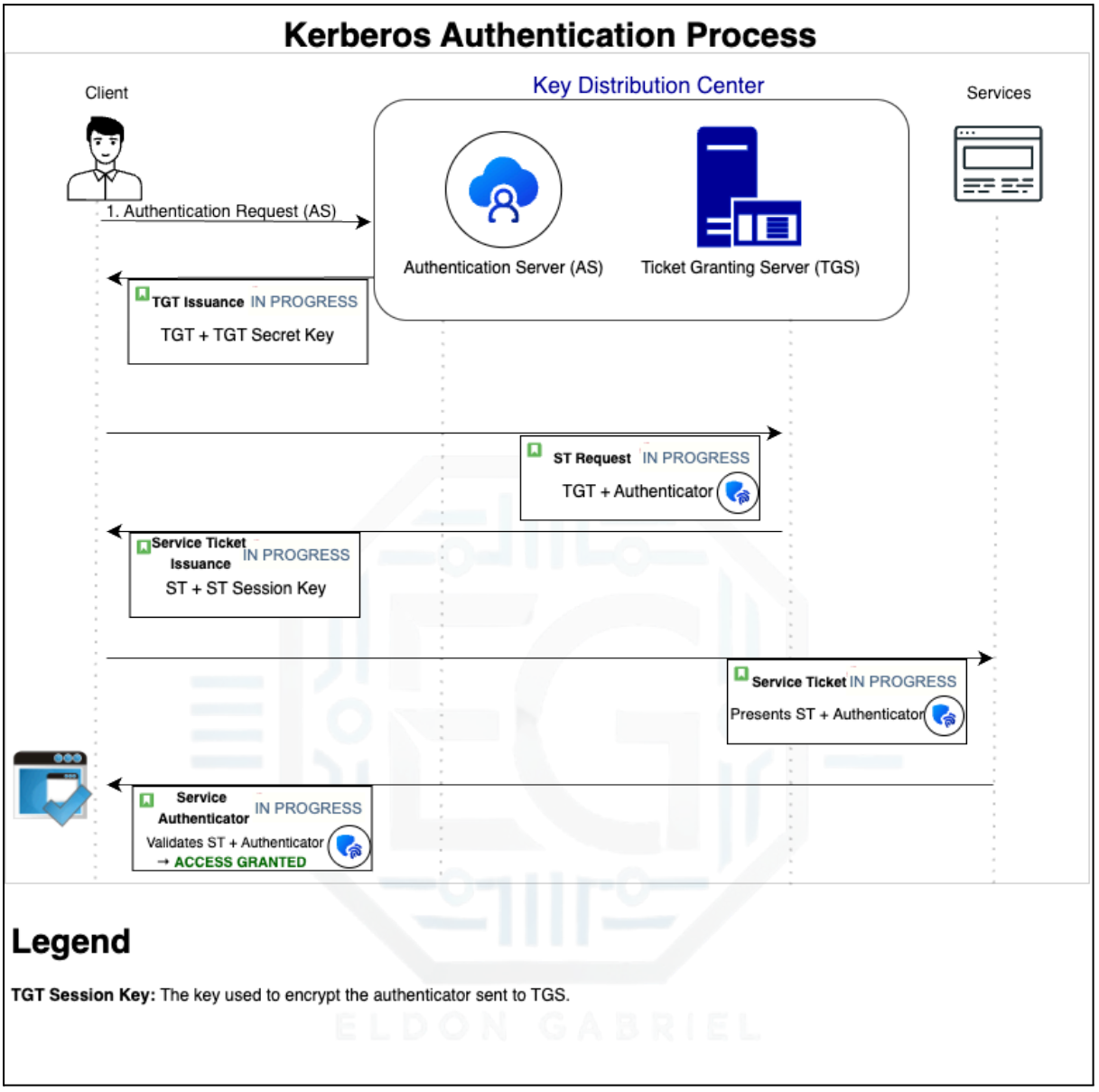


**Figure 2**: DIAGRAM - The Kerberos Authentication Process - v1.0.0. 2025. Eldon

## 3.7 Lifecycle of Kerberos Authentication Tickets

Kerberos authentication relies on a ticket lifecycle with two primary types of tickets: the Ticket-Granting Ticket (TGT) and the Service Ticket (ST). Each has a distinct purpose and lifecycle of creation, usage, and expiration.

### 3.7.1 Ticket-Granting Ticket (TGT)

- **Creation**: The TGT lifecycle begins when a client requests authentication from the **Authentication Server (AS**). The AS verifies the credentials and issues both a TGT and a session key. The TGT is encrypted with the Ticket Granting Service's (TGS) secret key, ensuring only the **Key Distribution Center (KDC)** can read it. The session key is encrypted with a key derived from the user's password.
- **Usage**: The client uses the TGT to request Service Tickets from the TGS without needing to send the password again. Each TGS request includes an authenticator, which is a timestamp and client information encrypted with the session key.
- **Expiration**: TGTs are time-limited, commonly lasting a few hours. Once a TGT expires, the client must request a new one from the AS to continue the authentication process.

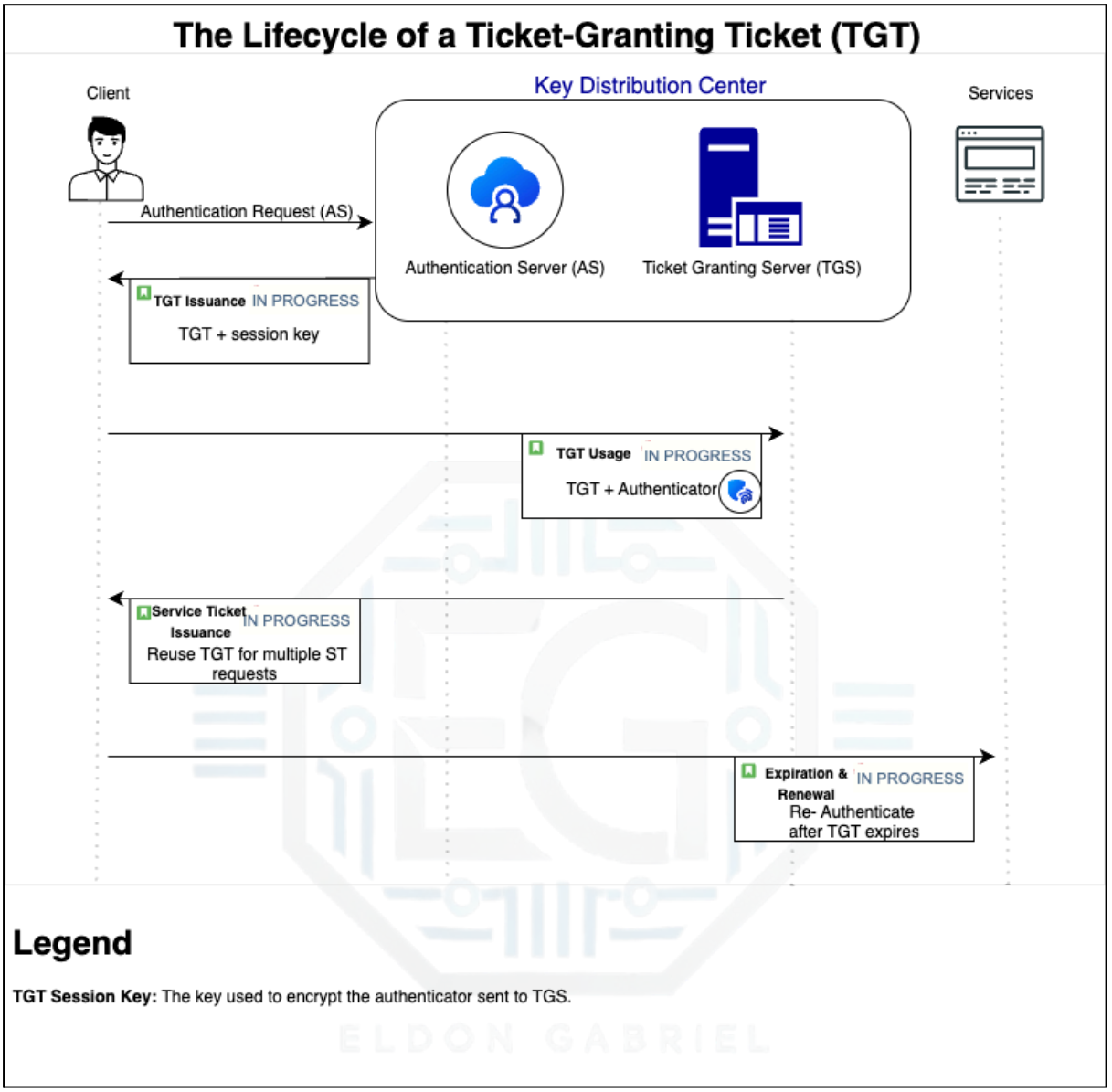


**Figure 3:** DIAGRAM - The Lifecycle of a Ticket-Granting Ticket (TGT) - v1.0.0. 2025. Eldon

## 3.7.2 Service Ticket (ST)

- **Creation**: A Service Ticket is created when the TGS issues an ST after validating the TGT and the authenticator. The ST is encrypted with the target service's secret key, and a new session key is generated for secure communication between the client and the service.
- **Usage:** The client presents the ST, along with a new authenticator, to the target service to gain access. The session key is then used to establish an encrypted communication channel between the client and the service.
- **Expiration**:Service tickets are also temporary and typically have a shorter lifespan than TGTs. Once an ST expires, the client must use its valid TGT to request a new ST from the TGS.

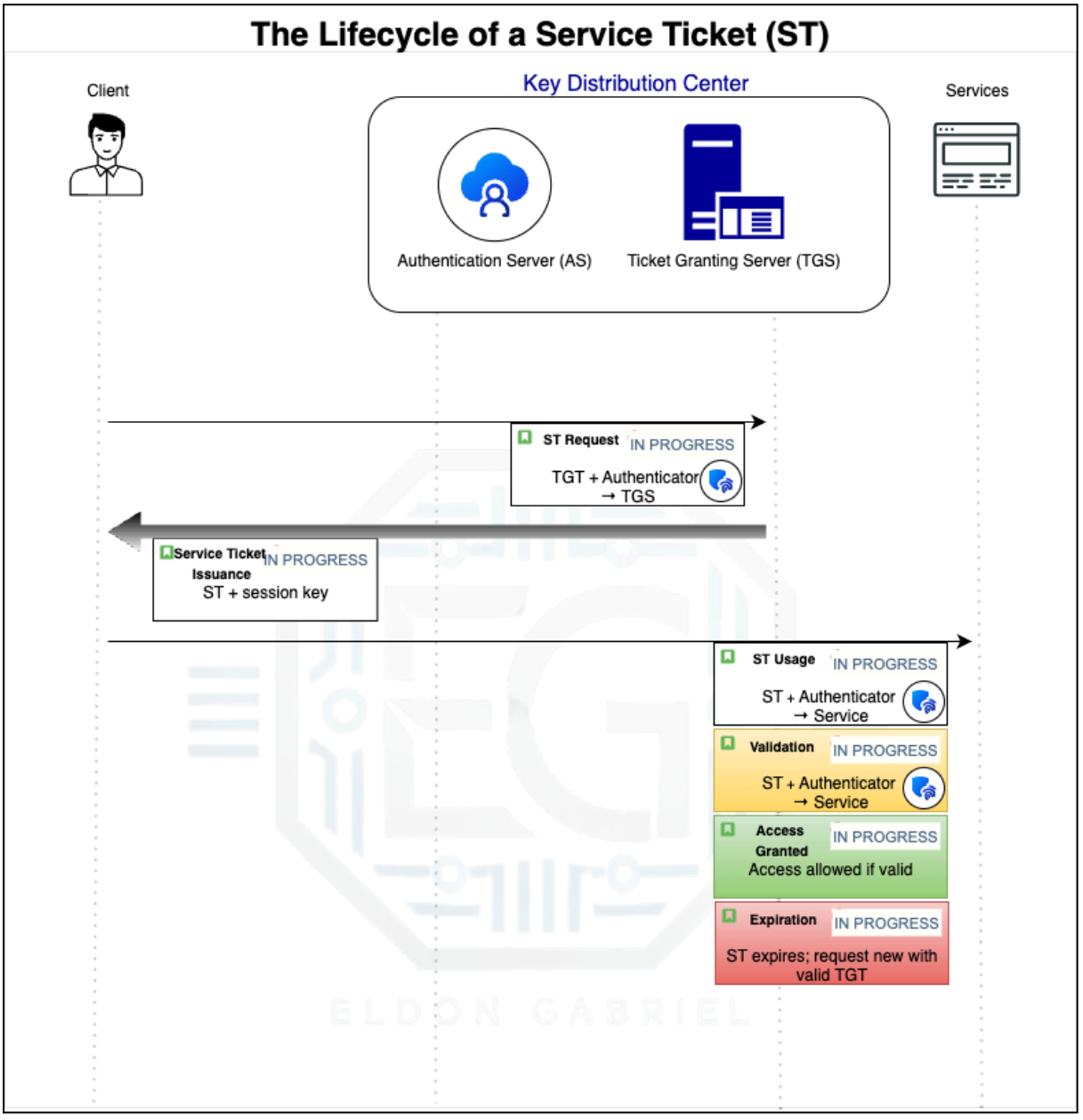


**Figure 4:** DIAGRAM - The Lifecycle of a Service Ticket (ST) - v1.0.0. 2025. Eldon

## Key Notes

The TGT session key is the key used to encrypt the authenticator sent to the TGS. The ST session key is used to encrypt communications with the target service.

---

# 4.0 SECURITY STRENGTHS OF KERBEROS

- **Symmetric-Key Cryptography:** Kerberos is built on shared keys between clients, servers, and the KDC. Because these keys are never sent over the network in clear text, the system minimizes the possibility of credential theft.
- **Single Sign-On (SSO):** Kerberos reduces login friction. After authenticating once, users can move between multiple services without typing their password again, thereby strengthening both security and usability.
- **No Plain-Text Passwords:** Passwords are never sent in their raw form. Instead, tickets and session keys act as cryptographic proof of identity, which keeps credentials safe during transmission.

---

# 5.0 VULNERABILITIES AND ATTACK VECTORS

- **Kerberoasting:** Attackers extract service tickets to brute force passwords offline.
- **Golden Ticket Attack:** Compromising the KDC master key allows attackers to forge ticket-granting tickets for unrestricted access.
- **Silver Ticket Attack:** Forging Service Tickets gives attackers access to specific resources without a TGT.

Understanding these risks highlights the importance of strong passwords, strict KDC protection, and active monitoring.

---

# 6.0 REAL-WORLD APPLICATION

## 6.1 Enterprise Integration

Kerberos is the default authentication protocol in enterprise environments, particularly within Microsoft Active Directory. It manages tickets, trust relationships, and access policies every time a user logs into the domain.

## 6.2 Practical Use Cases

- ➢ Accessing shared drives and internal applications.
- ➢ Email servers and collaboration platforms are also used.
- ➢ Secure SSO for cloud services and enterprise applications.

Kerberos also supports multifactor authentication and centralized logging for compliance.

---

# 7.0 CONCLUSION

Kerberos addresses the fundamental security problem of sending credentials across insecure networks. The use of encrypted, time-limited tickets and a centralized authentication authority reduces exposure to attacks, improves administrative control, and enables convenient Single Sign-On across enterprise resources.

---

# 8.0 PERSONAL ANALYSIS AND INSIGHTS

Studying Kerberos provides insights into how cryptography and careful system design can solve core cybersecurity challenges. Key points:

- **Centralization:** Simplifies policy enforcement and access control for users.
- **Security through Design:** Short-lived tickets and symmetric encryption protect credentials.
- **Usability and Security:** Single Sign-On balances convenience with strong protection.
- **Vulnerability Awareness:** Understanding attacks such as Kerberoasting and Golden/Silver Ticket attacks emphasizes the need for monitoring, strong passwords, and KDC security.

Kerberos demonstrates that effective authentication is about more than encryption—it is about building a system where credentials are never exposed and access control scales securely across an organization.

---

# DIAGRAMS

The following figures illustrate the key components and processes of the Kerberos authentication system.

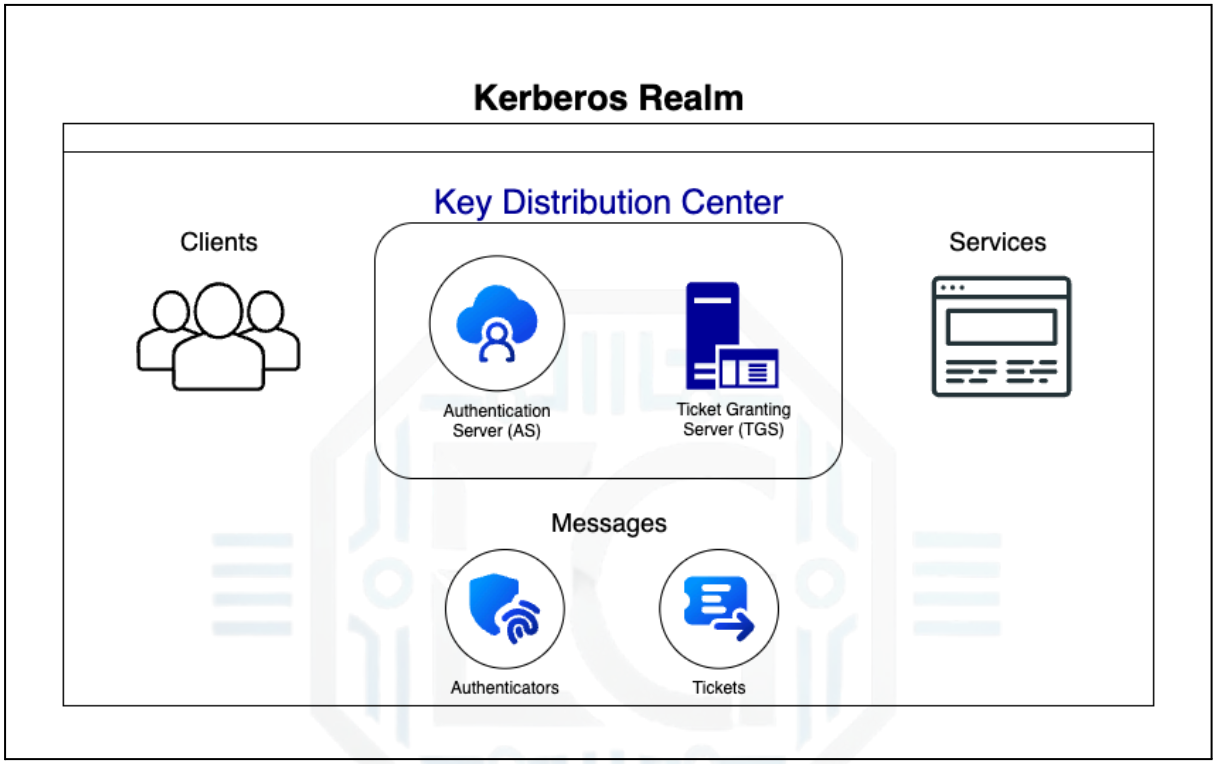


**Figure 1**: DIAGRAM - Kerberos Realm Components - v1.0.0. 2025. Eldon

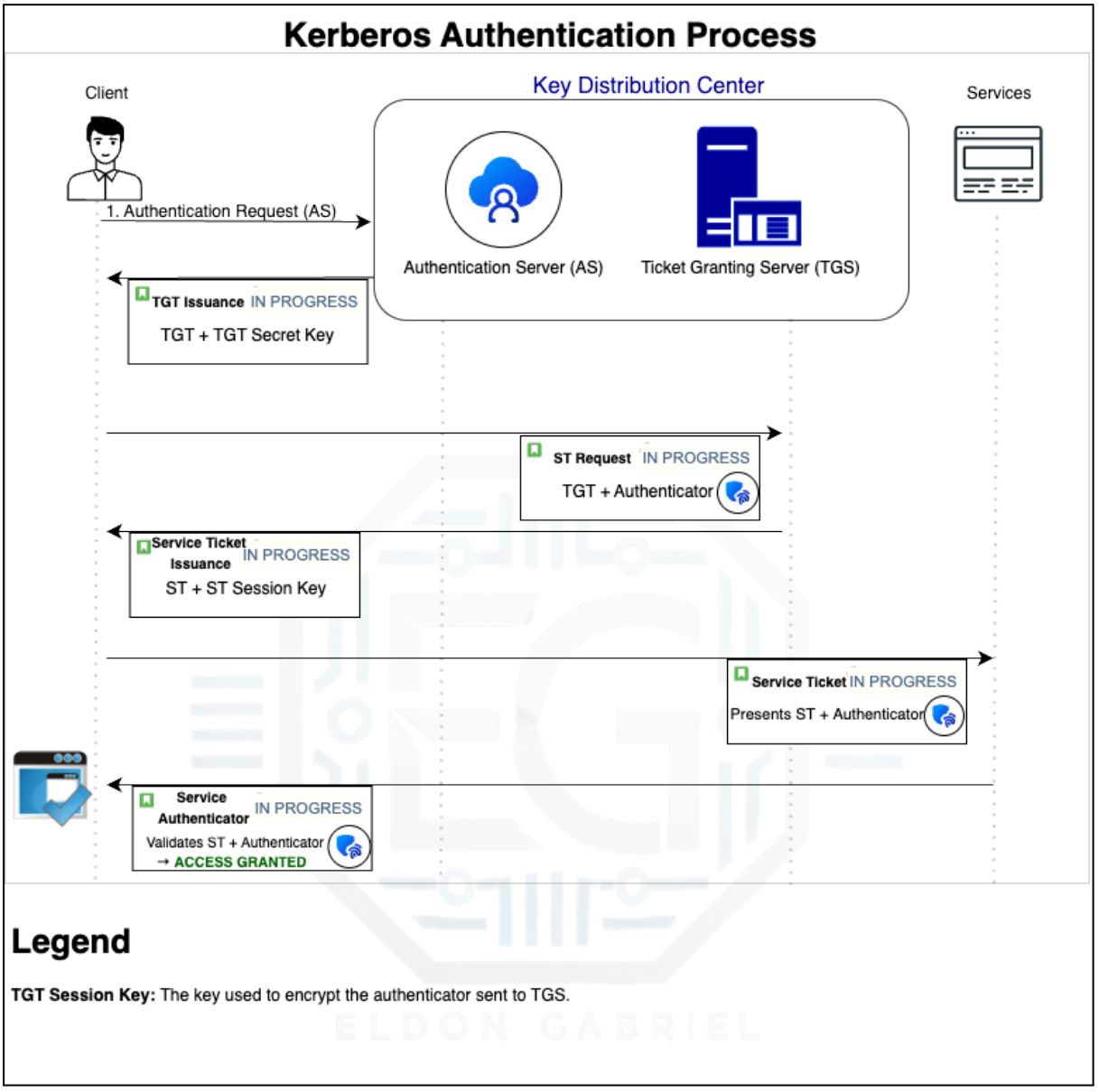


**Figure 2**: DIAGRAM - The Kerberos Authentication Process - v1.0.0. 2025. Eldon

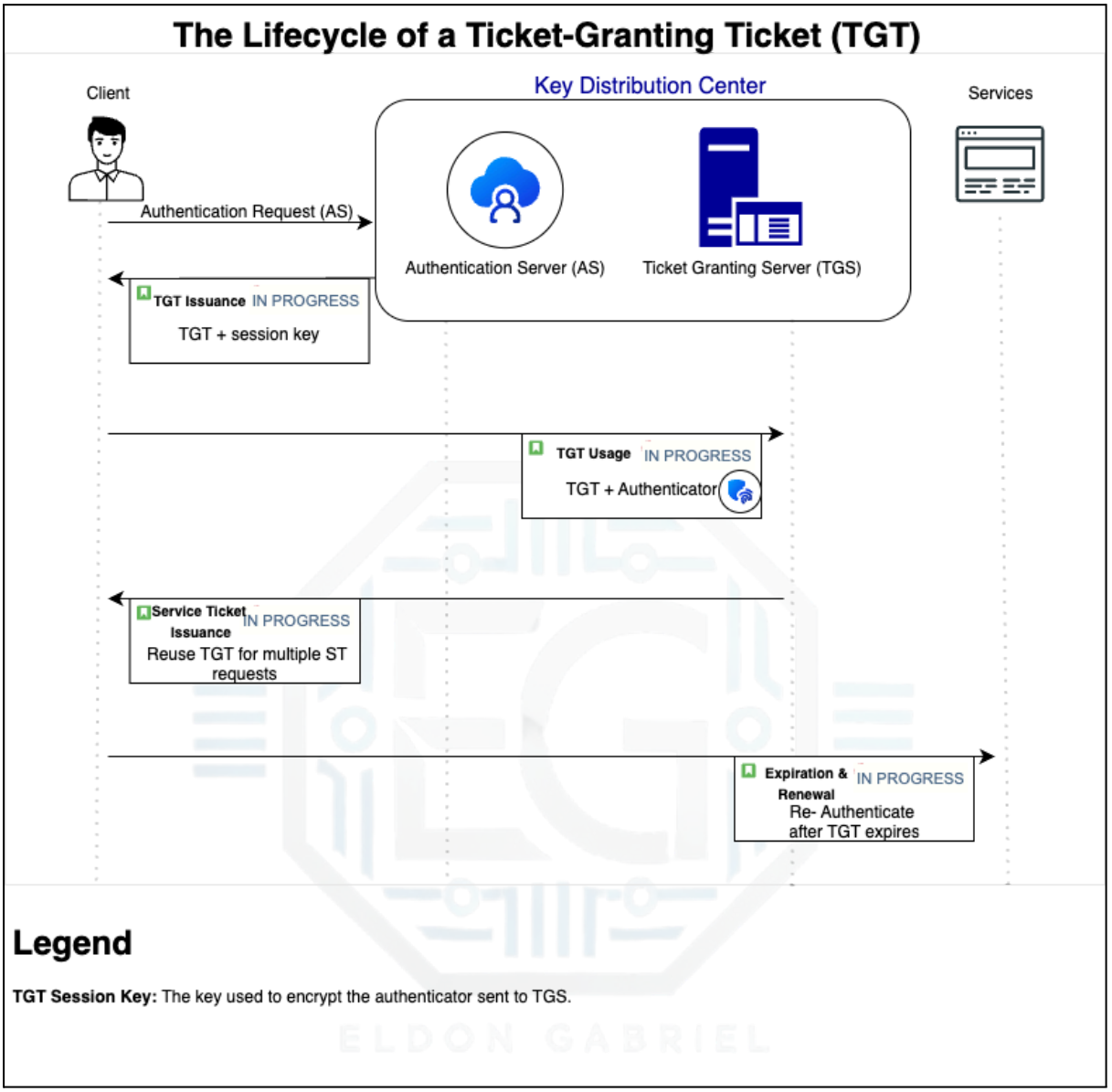


**Figure 3:** DIAGRAM - The Lifecycle of a Ticket-Granting Ticket (TGT) - v1.0.0. 2025. Eldon

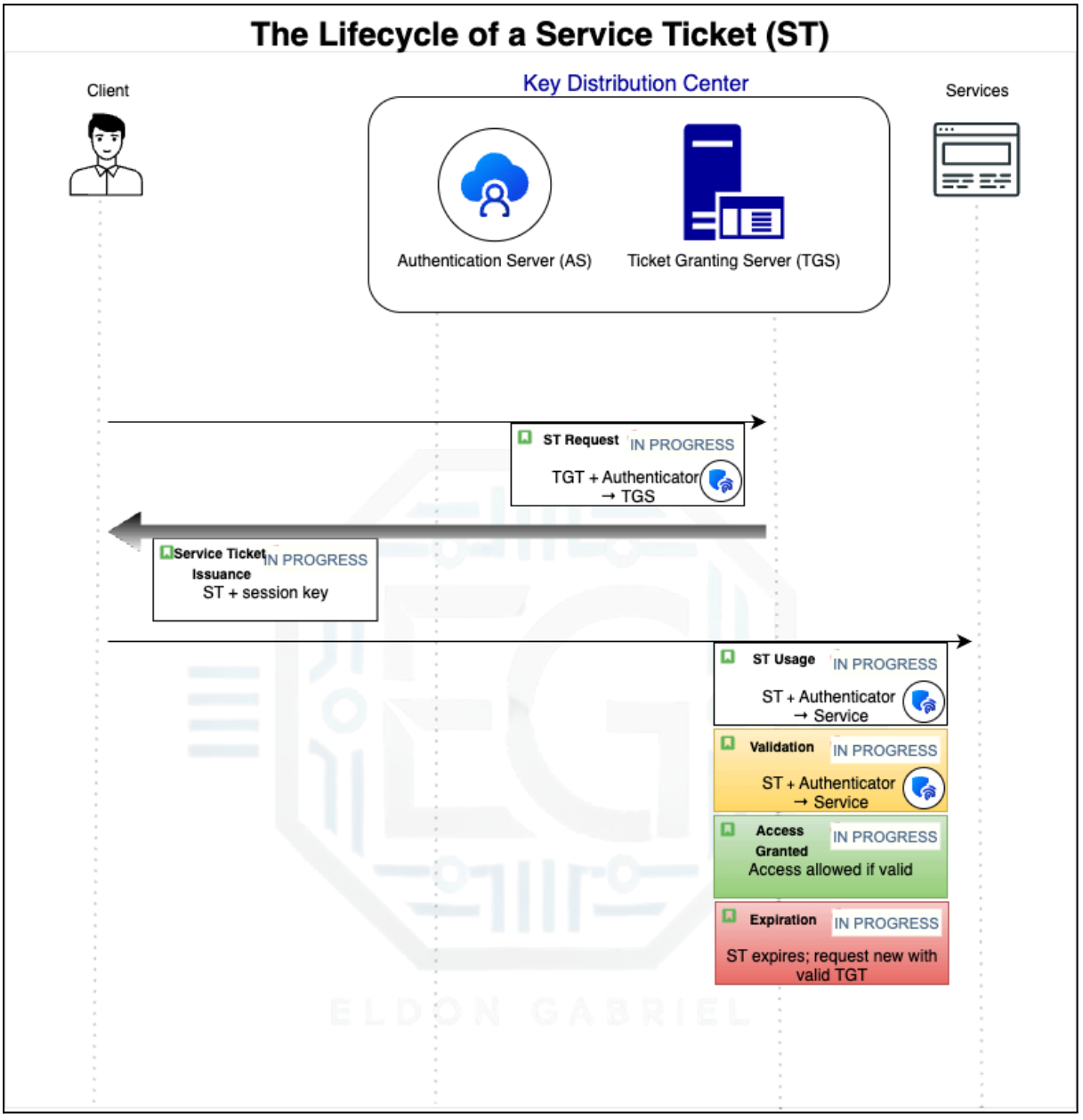


**Figure 4:** DIAGRAM - The Lifecycle of a Service Ticket (ST) - v1.0.0. 2025. Eldon