Seguridad en Redes de Comunicación

Tema II. Autentificación y Gestión de Claves

Jorge Lanza Calderón

Luis Sánchez González

Departamento de Ingeniería de Comunicaciones
Grupo de Ingeniería Telemática

Índice

- Qué es la autenticación
- Modelos de autenticación
  - Intercambios de autenticación
- Gestión de claves
  - Generación
  - Metodologías de distribución
- Kerberos
- Certificación digital - Infraestructura de clave pública
  - Certificado
  - Gestión de certificados
  - Uso de certificados
  - Marco legal

Índice

- Qué es la autenticación
- Modelos de autenticación
  - Intercambios de autenticación
- Gestión de claves
  - Generación
  - Metodologías de distribución
- Kerberos
- Certificación digital - Infraestructura de clave pública
  - Certificado
  - Gestión de certificados
  - Uso de certificados
  - Marco legal

Conceptos generales

Qué es la autenticación

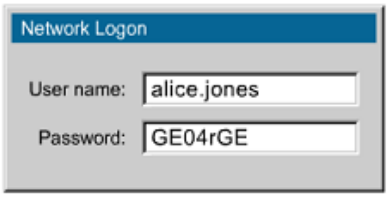
- Proceso de verificación de la identidad declarada por una entidad (persona, cosa, sistema, etc.)
  - Identificación: presentar una credencial al sistema de seguridad
  - Verificación: presentar o generar información que corrobora el vínculo entre la credencial y la entidad que quiere autenticarse
- Autenticación de mensajes ≠ Autenticación de personas
  - Autenticar un mensaje es verificar que el contenido de un mensaje no ha sido alterado y que la fuente es auténtica y válida
- Dos niveles
  - Autenticar al usuario o entidad que accede al sistema
  - Autenticar al proveedor o sistema
- Entornos de aplicación
  - Entornos atendidos
  - Entornos desatendidos

Conceptos generales

- Mecanismos
  - Algo que el individuo o entidad sabe
    - Clave, PIN, respuestas a preguntas, etc.
  - Algo que el individuo o entidad posee
  - Algo que el individuo o entidad es
  - Algo que el individuo o entidad hace
    - Acción
    - Localización
    - …
- Metodologías
  - Sistemas autenticados por clave
  - Sistemas autenticados por sus características
    - Dirección de red, etc.
  - …
  - Autenticación criptográfica

Mecanismos

- Claves de usuario
  - Número de identificación personal
  - Números y letras



- Biometría
  - Huella dactilar, geometría mano, voz, iris, reconocimiento facial, etc.
- Sistemas Single Sign-On (SSO)
  - Kerberos (criptografía simétrica)
  - SESAME (criptografía asimétrica)

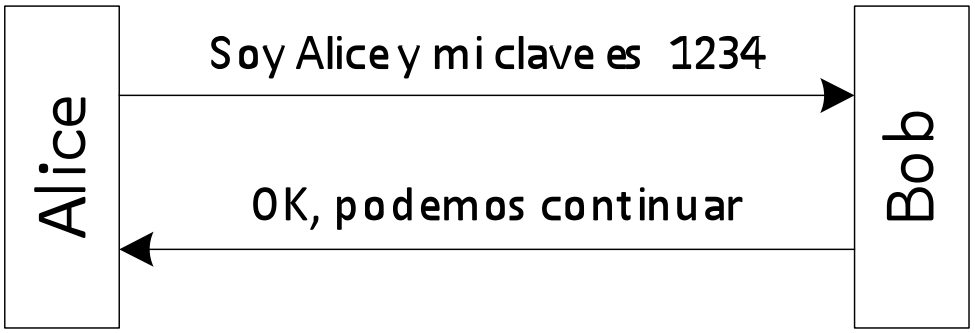
- Claves de un solo uso
  - Basadas en un token de autenticación
    - Síncrono o asíncrono

Índice

- Qué es la autenticación
- Modelos de autenticación
  - Intercambios de autenticación
- Gestión de claves
  - Generación
  - Metodologías de distribución
- Kerberos
- Certificación digital - Infraestructura de clave pública
  - Certificado
  - Gestión de certificados
  - Uso de certificados
  - Marco legal

Autenticación empleando claves

- Clave: secreto conocido que expones para probar que lo conoces

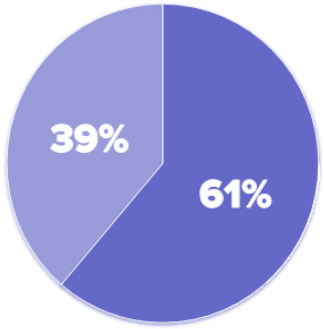


- Sistemas poco robustos ante ataques
  - En tiempo de ejecución: escucha (key loggers, video,...),prueba y error,...
    - Mecanismo del santo y seña
    - Hacer lento el proceso
    - Numero de intentos limitado en total, por sesión, …
  - Fuera de línea: diccionario, lectura ficheros, …
    - Claves robustas y variables
    - One-Time-Password (OTP)

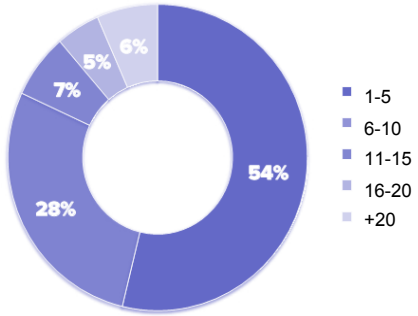
Autenticación empleando claves

Modelos de autenticación

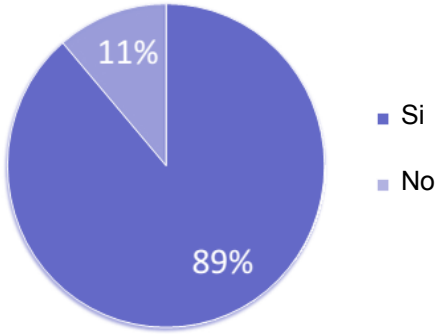
- Características del usuario



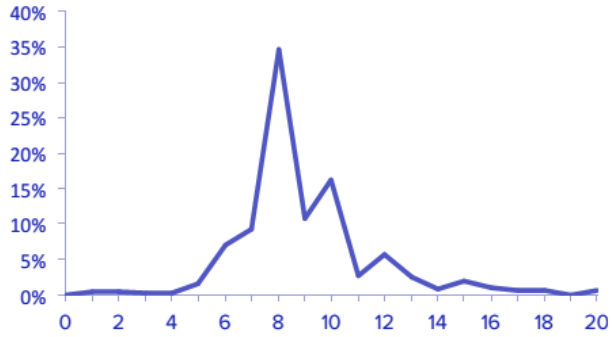
Modo de uso



Número de claves



Apreciación seguridad



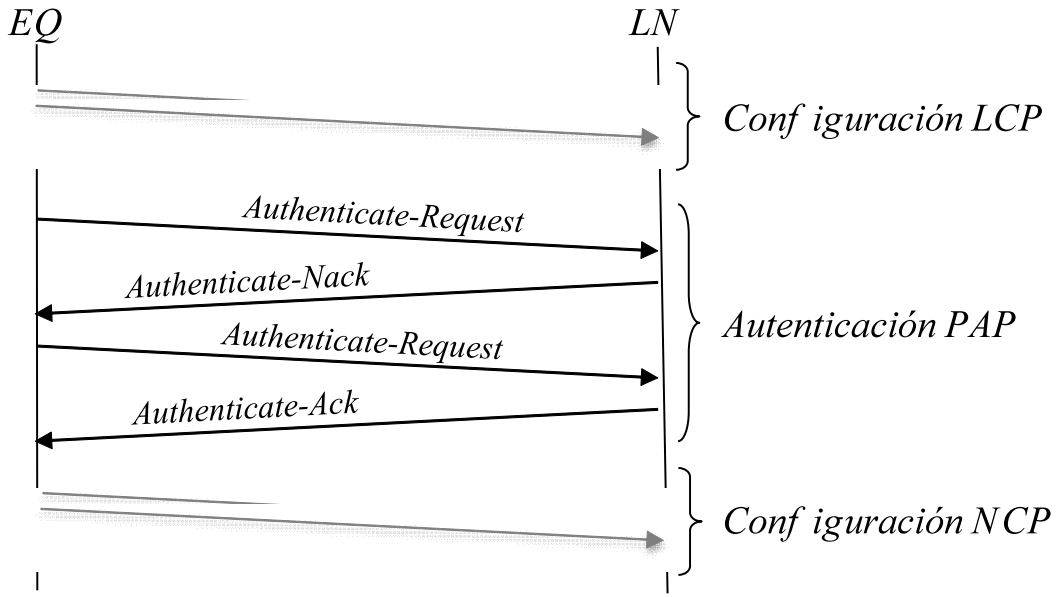
Longitud de clave

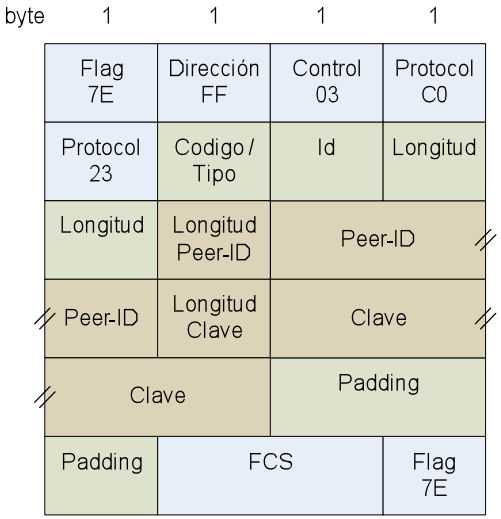
  - 60% personas usan clave sencillas (no aleatorias ni únicas) ESET 2012 Rainbow 2003
  - 55% usuarios escribe su clave al menos una vez Rainbow 2003
  - 40% usuarios cambia su clave al menos una vez al año en su vida Rainbow 2003
  - 32% de 6M personas usan la clave 123456 Stricture Top 100 2013

- Características de los sistemas
  - 50% compañías comparten clave administrador entre empleados 2013
  - Sistemas complejos con características desconocidas para usuarios

Autenticación empleando claves

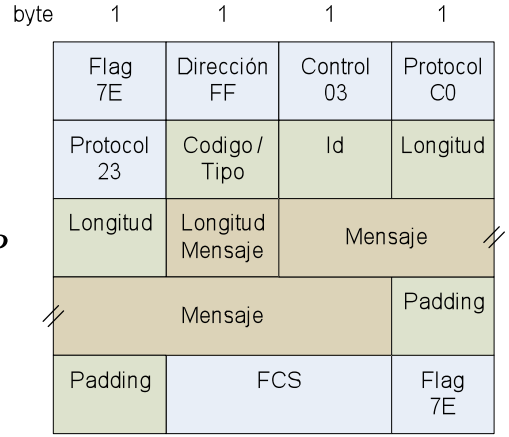
- Password Authentication Protocol
  - Transmite claves en ASCII en claro





Authenticate-Request

Authenticate-Request	01
Authenticate-Ack	02
Authenticate-Nack	03



Authenticate-Ack/Nack

Autenticación criptográfica

- Protocolos son más seguros que otras alternativas
  - Agregan variabilidad
  - Independencia del usuario
- Herramientas empleadas
  - Hashes o funciones resúmenes
  - Criptografía de clave simétrica o asimétrica
- Gestión de la claves
  - Generación
  - Distribución y actualización
  - Almacenaje
  - Destrucción

Generación de la clave

- La seguridad de un sistema criptográfico reside en la clave y no en el algoritmo
  - Ocultar la clave de alguna forma

- Robustez de la clave (estimación de validez según la longitud en http://www.keylength.com/)
  - Depende de la información que cifre
    - Mayor longitud, más tiempo, más energía
  - Evitar generación por parte de un usuario
    - Cifrado de la clave criptográfica
  - Depende de algoritmo criptográfico empleado
  - Fuerza bruta ⇒ tiempo vs coste
    - Seguridad es exponencial y no doble
    - Ley de Moore: potencia de cálculo
    - Paralelización del cálculo
  - Variabilidad de la clave ⇒ derivación de claves

$2^{56} = 72057594037927936 = 7.206 \cdot 10^{16}$

$2^{128} = 3.403 \cdot 10^{38}$

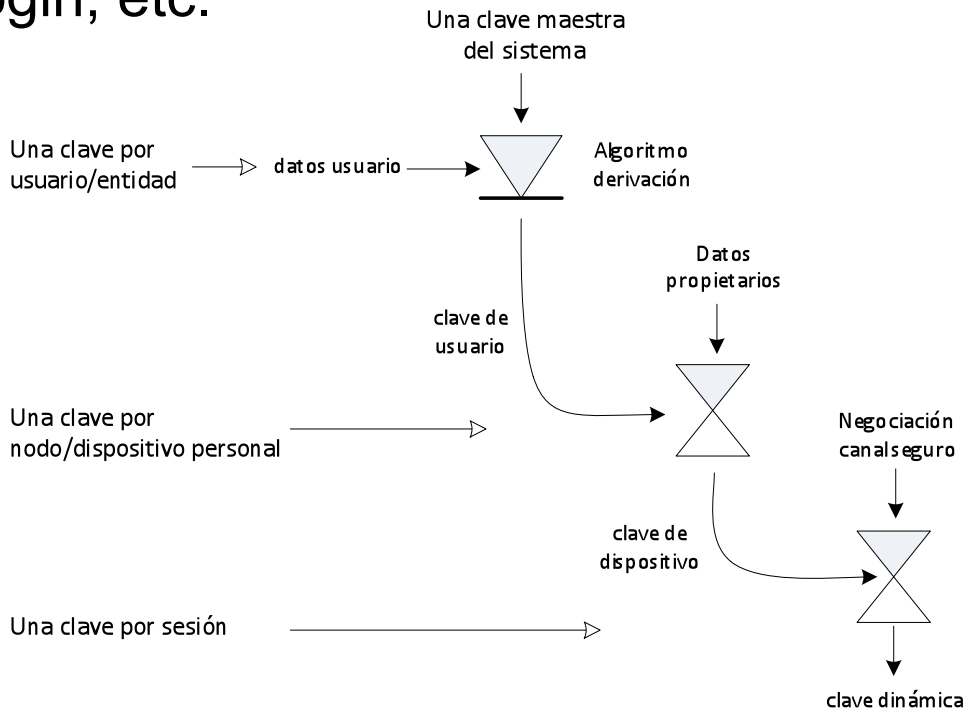
$2^{2048} = 3.232 \cdot 10^{616}$ a factorizar n=pq

Simétrica	Asimétrica
80 bits	1024 bits
112 bits	2048 bits
128 bits	3072 bits

Equivalencia claves

Distribución inicial de las claves

- Envío físico de claves a los usuarios
- Entidades de confianza
  - Autenticar al receptor por medios externos
- Claves de un solo uso
  - Necesidad de cambiarlas tras primer login, etc.
- Claves usadas para actualización
- Tokens seguros
  - Tarjeta inteligente
    - Tarjeta chip, SIM, tarjeta bancaria, etc.
  - Generador de números sincronizado
- Jerarquía de claves
  - Claves maestras
  - Claves de sesión



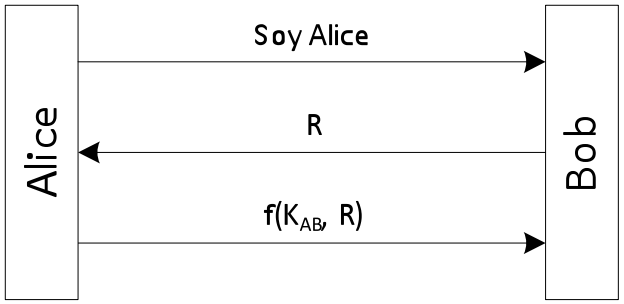
Modelos básicos

- Autenticación interna
  - Validación de la identidad de una entidad ante el resto del mundo
- Autenticación externa
  - Validación de la identidad del resto del mundo ante una entidad
- Autenticación mutua
  - Dos entidades se autentican entre sí y validan su identidad

Modelos básicos

- Autenticación interna y externa
  - Mejora con respecto a empleo de claves en claro

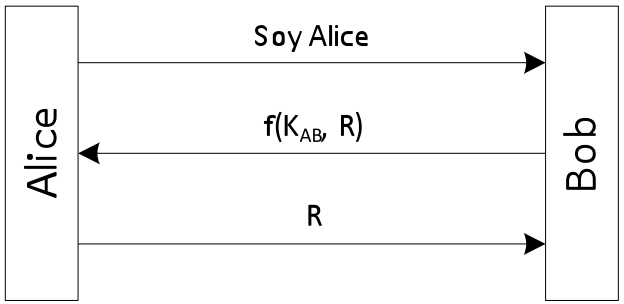
¿Es Bob o Mallory?



Es Alice

  - Características de f(x,y)
    - Cualquier tipo de función: cifrado, hash, etc.

¿Es Bob o Mallory?



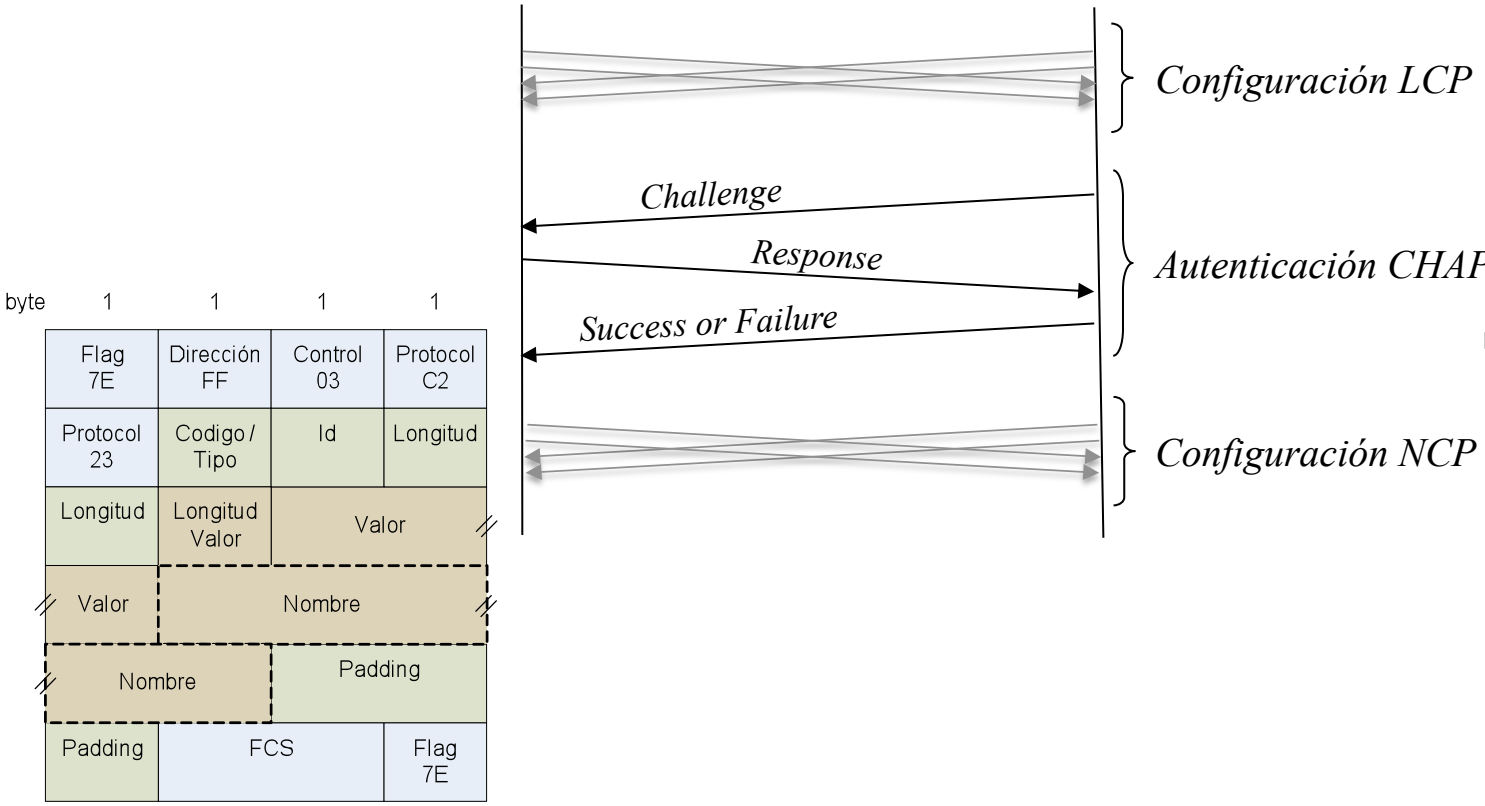
Es Alice

  - Características de f(x,y)
    - Debe ser una función reversible

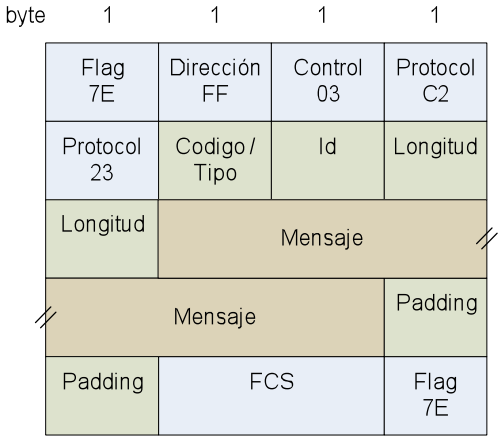
Modelos básicos

Autenticación criptográfica

- Protocolo Challenge Handshake Authentication Protocol



Challenge/Response

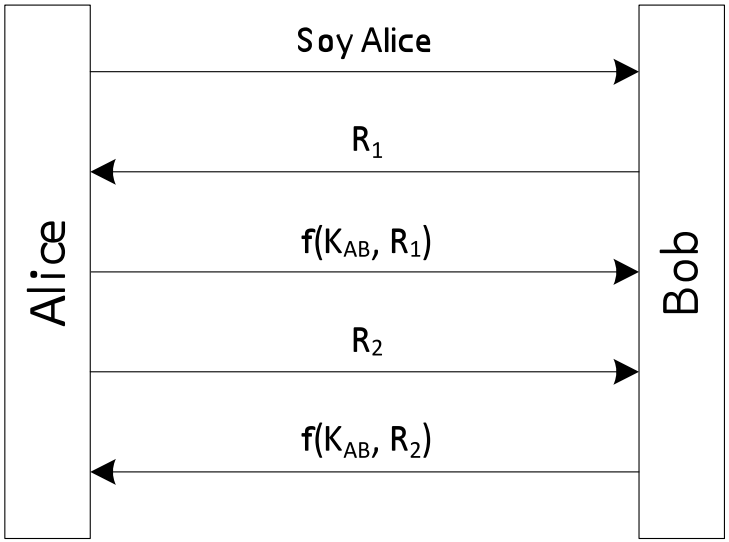


Success/Failure

Modelos básicos

- Autenticación mutua

Es Bob



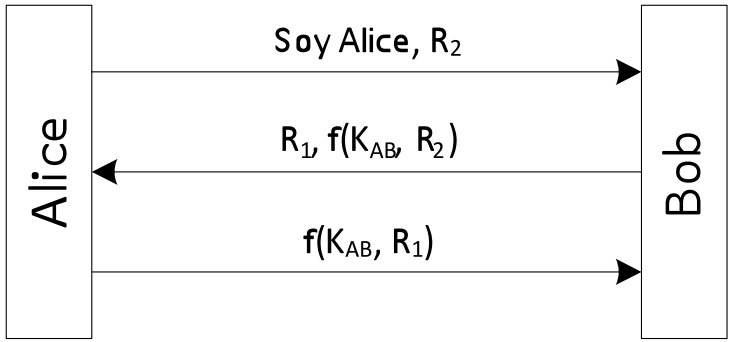
Es Alice

- Replicar la autenticación en ambos sentidos
- Protocolo planteado de forma ineficiente

Modelos básicos

- Autenticación mutua

Es Bob



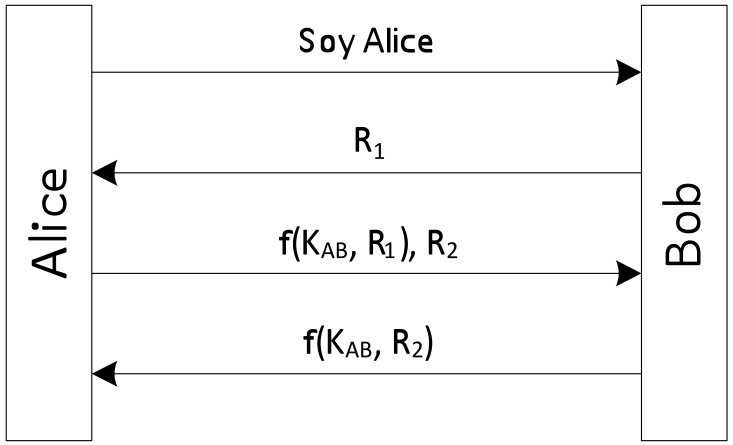
Es Alice

  - Ataque por reflexión
    - Metodología
      - Mallory remplaza a Alice obtiene R_2 firmado de Bob y R_1
      - Mallory reemplaza a Alice y envía R_1 obteniendo la respuesta $f(K_{AB}, R_1)$
      - Mallory es capaz de enviar a Bob $f(K_{AB}, R_1)$
    - Solución
      - $K_{AB} \neq K_{BA}$ o usar $f(K_{AB}, R_2 \,||\, ID_{BOB})$
  - Ataque por adivinación de clave

Modelos básicos

- Autenticación mutua

Es Bob



Es Alice

- Se obliga a que el potencial atacante inicie el proceso y de muestra de su identidad
- Propenso a reemplazo de identidad de Bob
  - Complicado de ejecutar

Modelos básicos

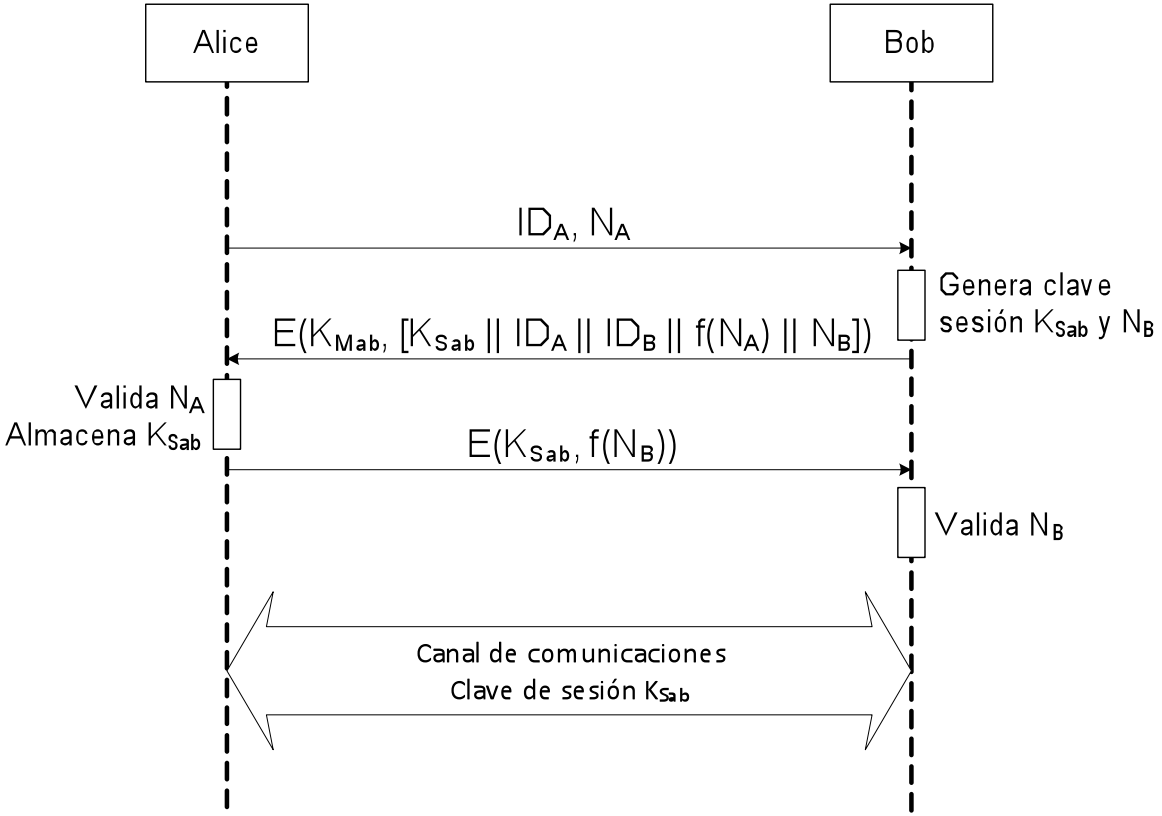
- Evitar los posibles ataques a la confidencialidad y temporalidad
  - Claves se comparten cifradas
- Ataques por temporalidad
  - Repetición simple: *copy & paste*
  - Repetición dentro de un periodo temporal
  - Mensajes no llegan a destino y se reemplazan por otros
  - Repuestas generadas a partir de mensajes guardados
- Variabilidad en la información en los intercambios
  - Sellos de tiempo
  - Challenge / Response
  - Contadores de operación
  - *Salt* (cadena aleatoria concatenada)
  - Claves de sesión de duración reducida

Índice

- Qué es la autenticación
- Modelos de autenticación
  - Intercambios de autenticación
- Gestión de claves
  - Generación
  - Metodologías de distribución
- Kerberos
- Certificación digital - Infraestructura de clave pública
  - Certificado
  - Gestión de certificados
  - Uso de certificados
  - Marco legal

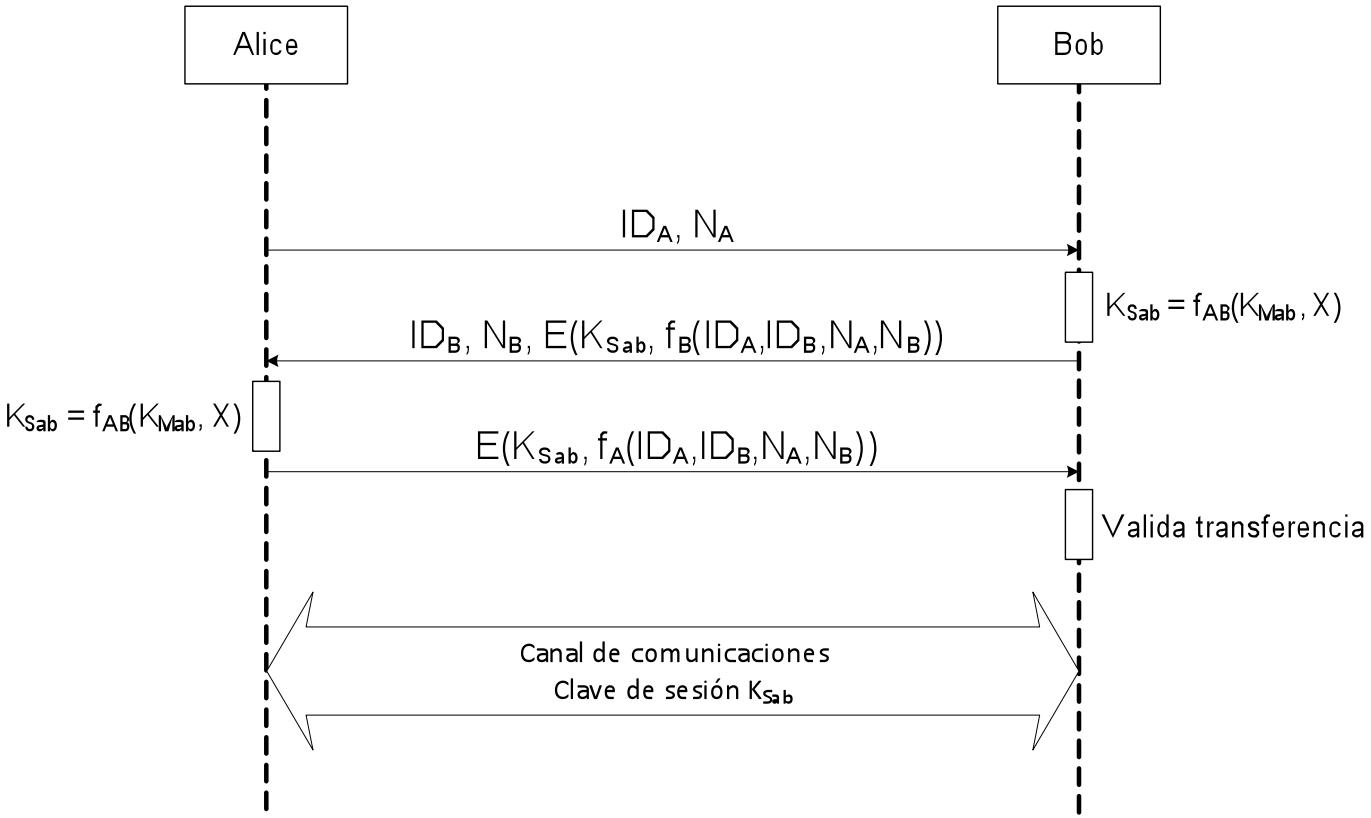
Distribución de claves

- Autenticación normalmente está vinculada a la distribución de claves
  - Autenticados los extremos de la comunicación, hay que asegurar la transferencia de información entre ellos

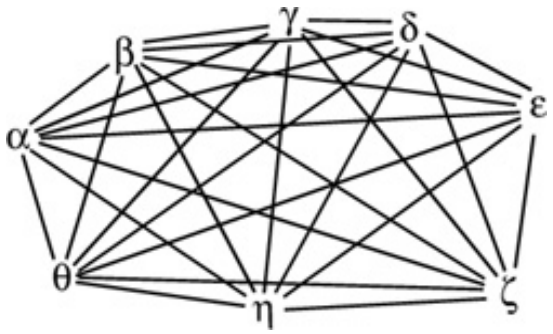


Distribución de claves

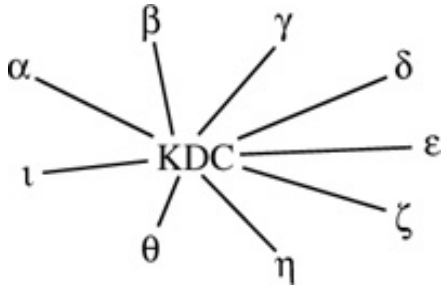
- Autenticación normalmente está vinculada a la distribución de claves
  - Autenticados los extremos de la comunicación, hay que asegurar la transferencia de información entre ellos



Distribución de claves



$$\text{Total claves} = \frac{n\,(n-1)}{2}$$



$$\text{Total claves} = n$$

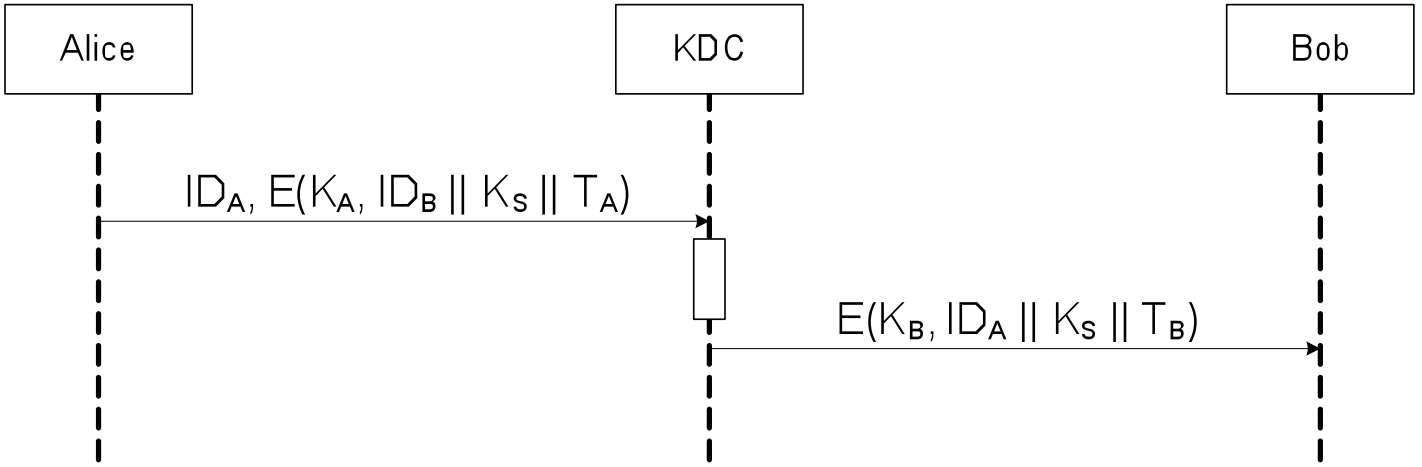
- ¿Cómo reducir el número de claves?
  - Gestión centralizada
  - Empleo de criptografía asimétrica (?)

Centro de distribución de claves

- Conocidos como KDC (*Key Distribution Centers*)
  - Todo el mundo debe de comunicarse con ellos
  - Siempre deben estar disponibles
- Operan en sistemas con múltiples usuarios con permisos variables de acceso a servicios
- Funcionalidades
  - Almacenamiento y distribución de claves
  - Servicio de autenticación
  - Tickets de acceso al servicio
- Emplean cifrado basado en algoritmos de clave simétrica
  - Claves específicas para la distribución provistas por KDC
- Problemas
  - Único punto de fallo y cuello de botella

Centro de distribución de claves

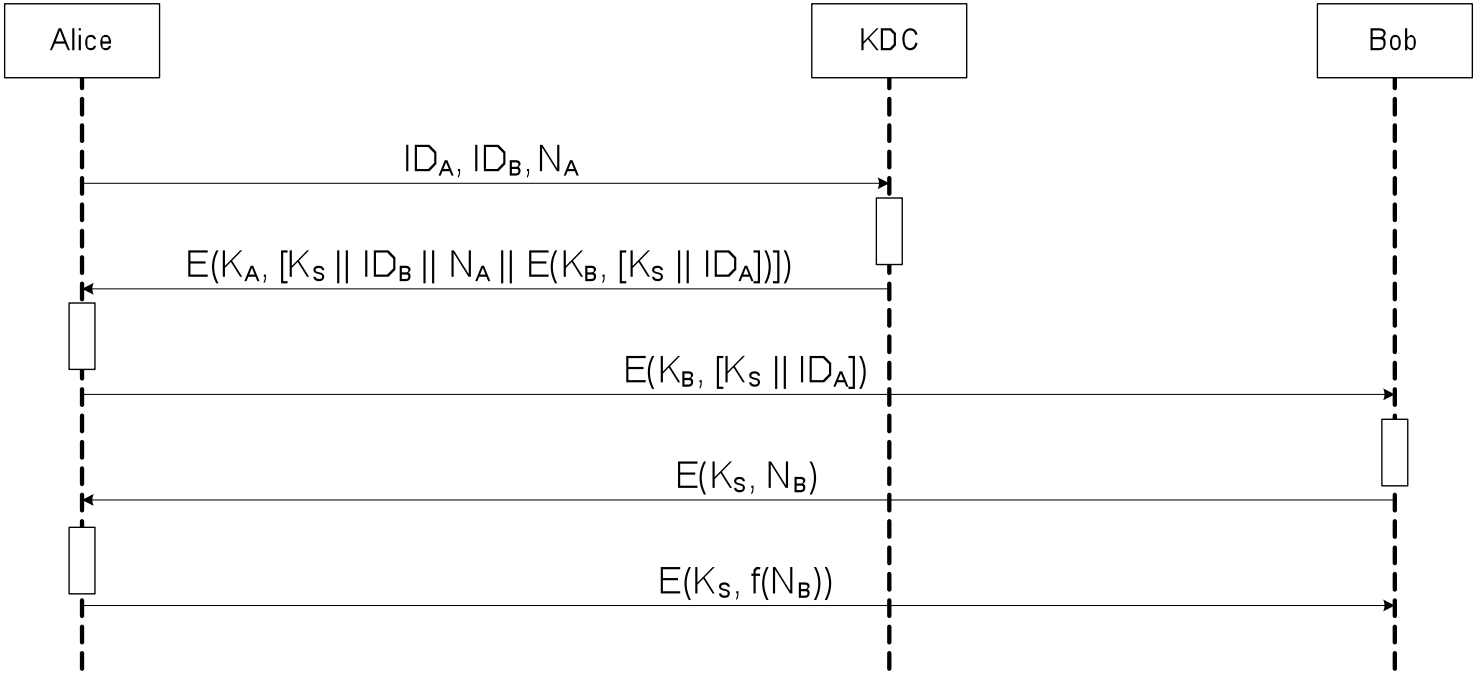
- White-Mouth Frog



  - Redirección de la información a través del KDC
  - K_S generada por Alice ⇒ La confianza del sistema recae en Alice

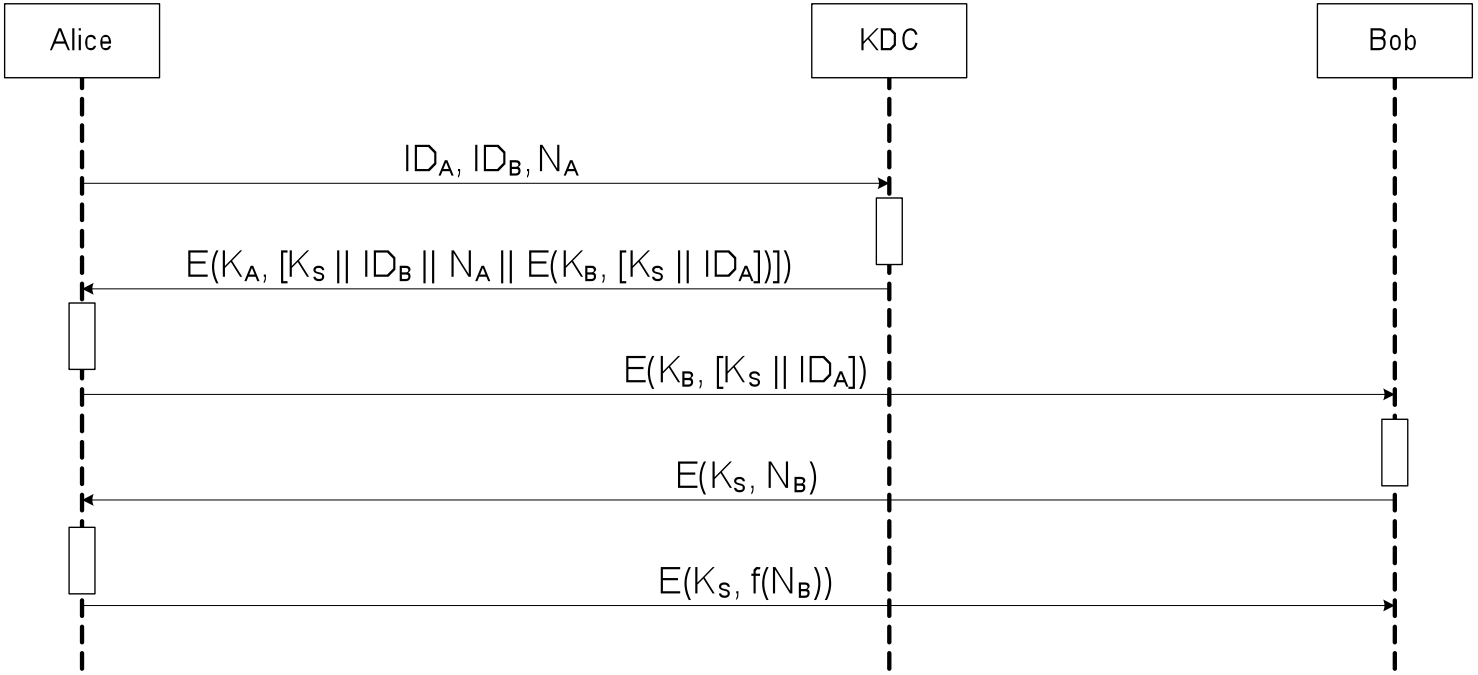
Centro de distribución de claves

- Needham-Schroeder



Centro de distribución de claves

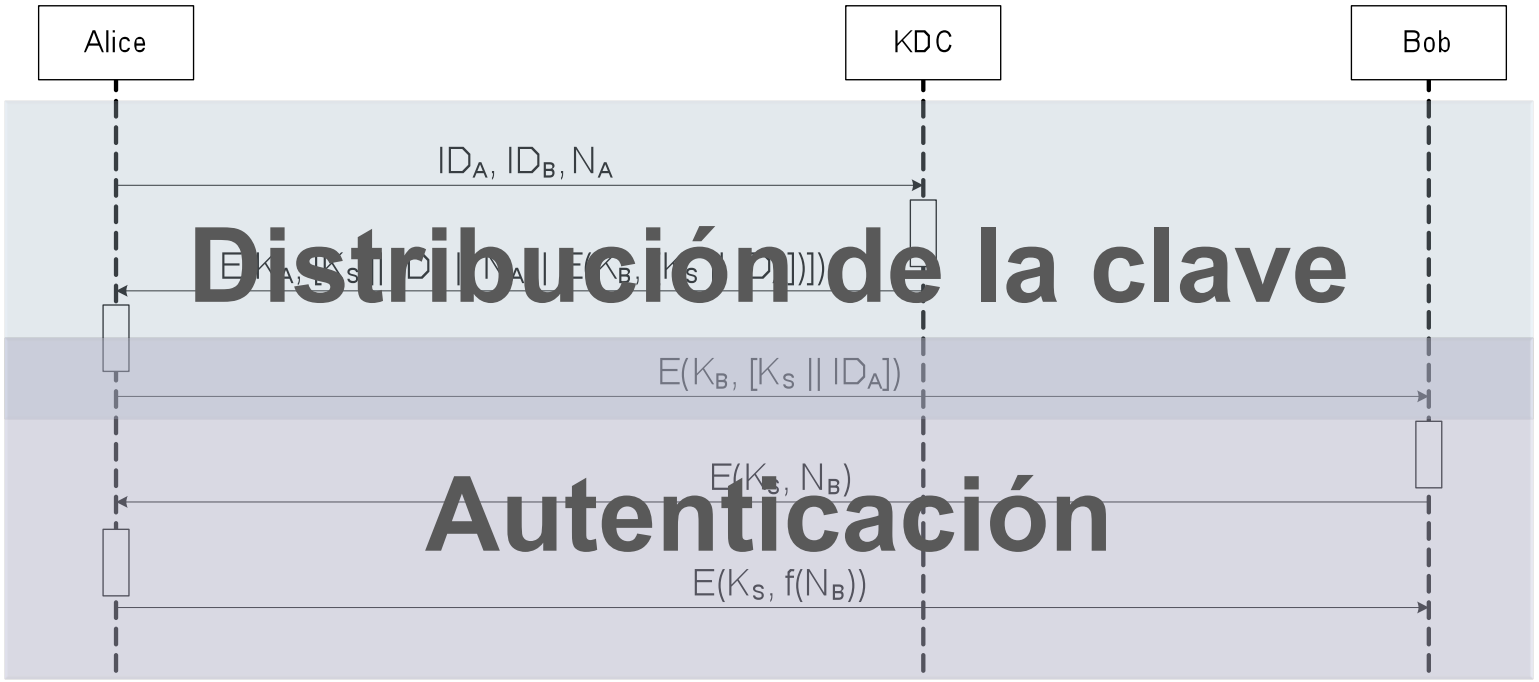
- Needham-Schroeder



- ¿Problemas?

Centro de distribución de claves

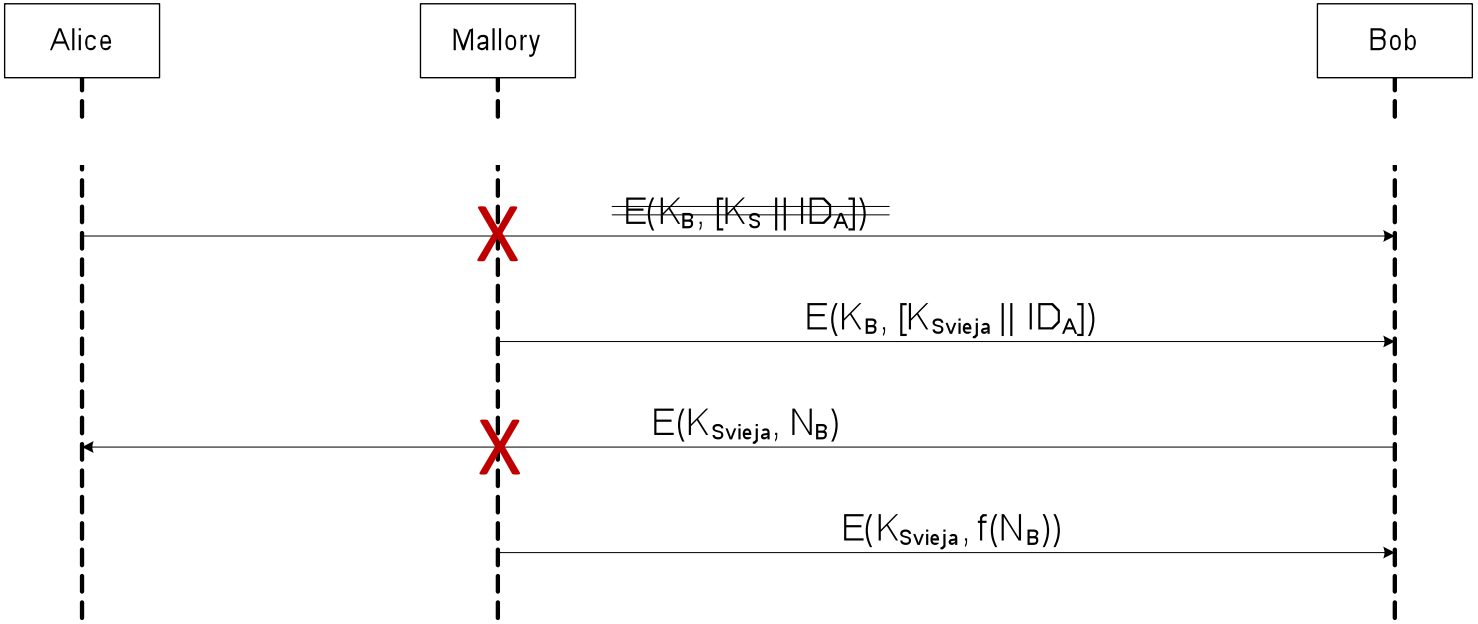
- Needham-Schroeder



- ¿Problemas?

Centro de distribución de claves

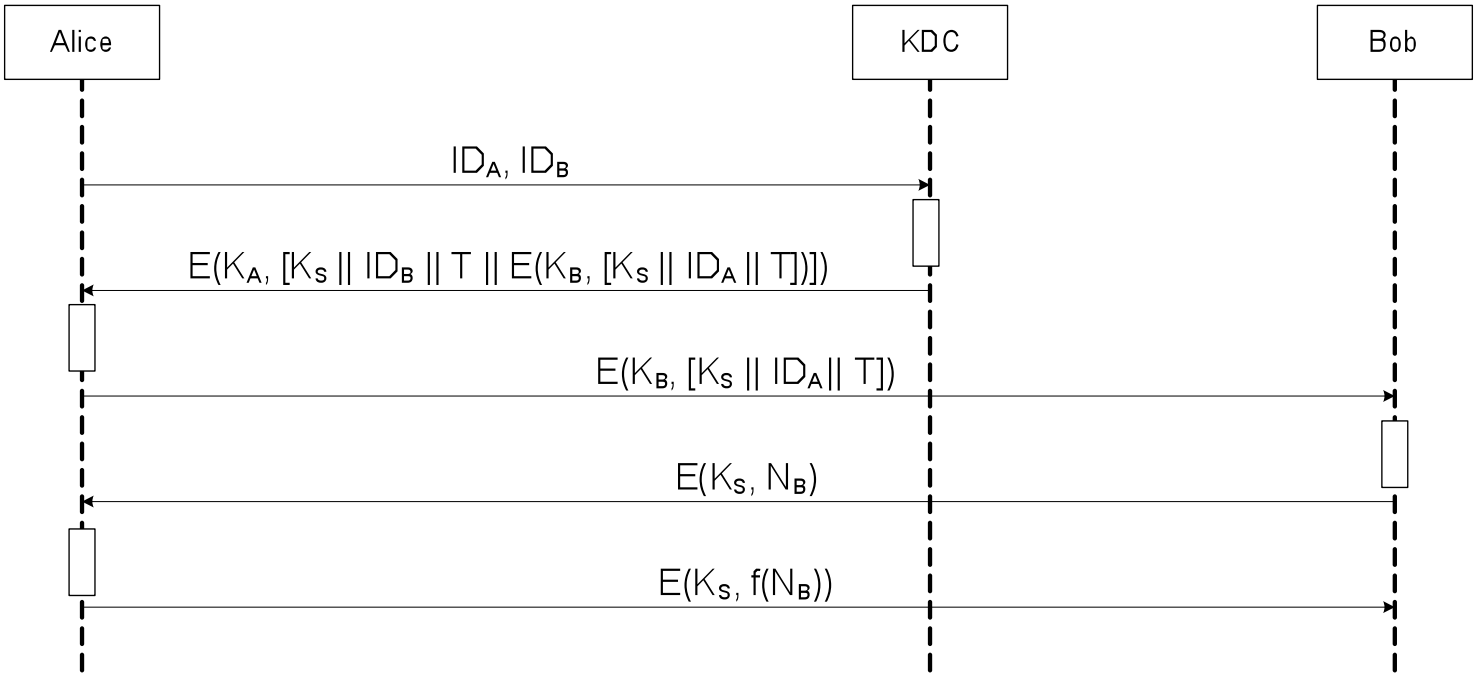
- Needham-Schroeder



- ¿Problemas? Sí, si Mallory tiene acceso a una clave ya usada
- ¿Solución?
  - Listado de claves usadas
  - Claves con una validez temporal

Centro de distribución de claves

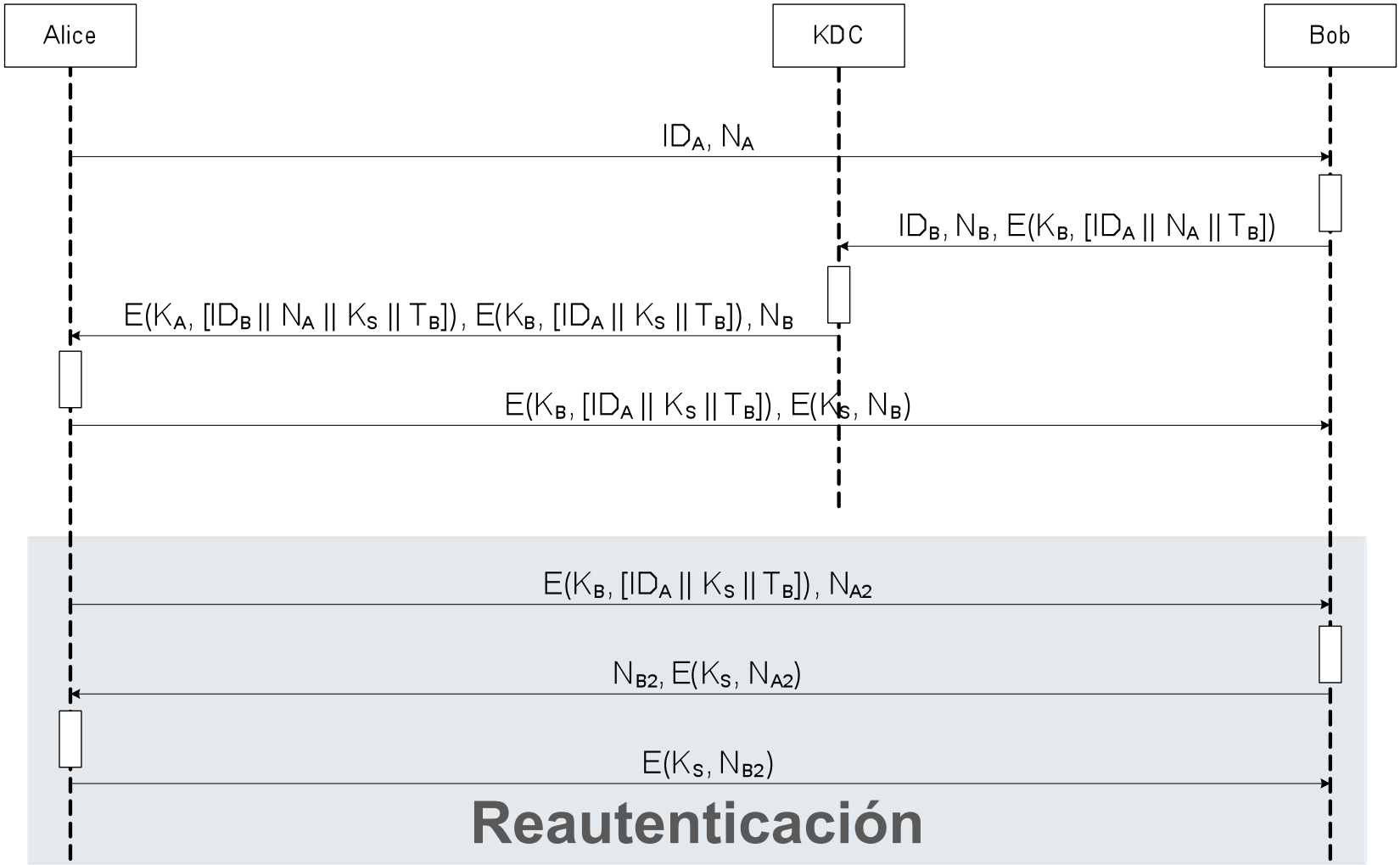
- Denning



- T es un sello de tiempo del momento en que se ha generado la clave K_S
- ¿Problemas? Sí, si reloj está adelantado al de Bob
  - Sincronizar relojes con el de KDC
  - Usar tiempos relativos y números aleatorios

Centro de distribución de claves

- Neuman-Stubblebine (Yahalom modificado)



Centro de distribución de claves

- Se ha observado que
  - KDC son necesarios para mantener la confianza en redes
  - La vida de las claves debe limitarse para mayor seguridad
  - Las claves no tiene un único propósito
    - Vincular la clave a un servicio, aplicación, etc.
    - Almacenar y gestionar las claves adecuadamente
- Escenario de uso
  - Red distribuida de equipos y servicios
  - Usuarios quieren acceder a los servicios
- Requerimientos
  - Seguro
  - Fiable y robusto
  - Transparente y amigable
  - Escalable

Índice

- Qué es la autenticación
- Modelos de autenticación
  - Intercambios de autenticación
- Gestión de claves
  - Generación
  - Metodologías de distribución
- Kerberos
- Certificación digital - Infraestructura de clave pública
  - Certificado
  - Gestión de certificados
  - Uso de certificados
  - Marco legal

Introducción

- Sistema de autenticación mutua / distribución de claves en red basado en la existencia de una tercera entidad de confianza
  - No garantiza que KDC, proveedores de servicios ni clientes están actualizados y a salvo de errores
- Desarrollado por MIT (proyecto Athena)

- Objetivos
  - Claves de usuario no circulen por la red
  - Claves de usuario no se almacenen en los equipos cliente
  - Claves de usuario almacenadas de forma cifrada en KDC
  - Administración centralizada
  - Usuario introducirá su clave una vez por sesión (SSO)
  - Autenticación mutua de cliente y servicios
  - Establecer un canal seguro

Introducción

- Sistema de autenticación mutua / distribución de claves en red basado en la existencia de una tercera entidad de confianza
  - No garantiza que KDC, proveedores de servicios ni clientes están actualizados y a salvo de errores
- Desarrollado por MIT (proyecto Athena)

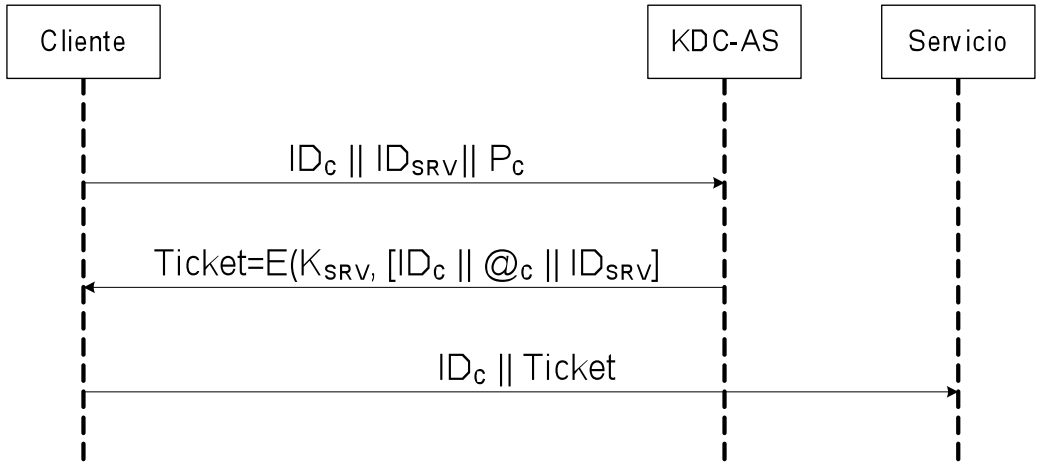
- Proporciona 3 niveles de seguridad
  - Autentificación al inicio de la conexión
  - Autentificación de los mensajes, mensaje seguros
  - Autentificación y privacidad de los mensajes, mensajes privados.

Evolución

- Basado en protocolo Needham-Schroeder
- Versión 4
  - Simple y buen rendimiento
  - Soporte solo sobre redes TCP/IP y empleo de DES
- Versión 5 (RFC 4120)
  - Elimina limitaciones de v4
    - Independencia de la red subyacente
    - Estandariza procedimientos y representación de la información
  - Mejora el tratamiento de la seguridad de v4
    - Algoritmos de cifrado
    - Eficiencia
    - Soporte multi-dominio y multi-autenticación

Construcción del protocolo

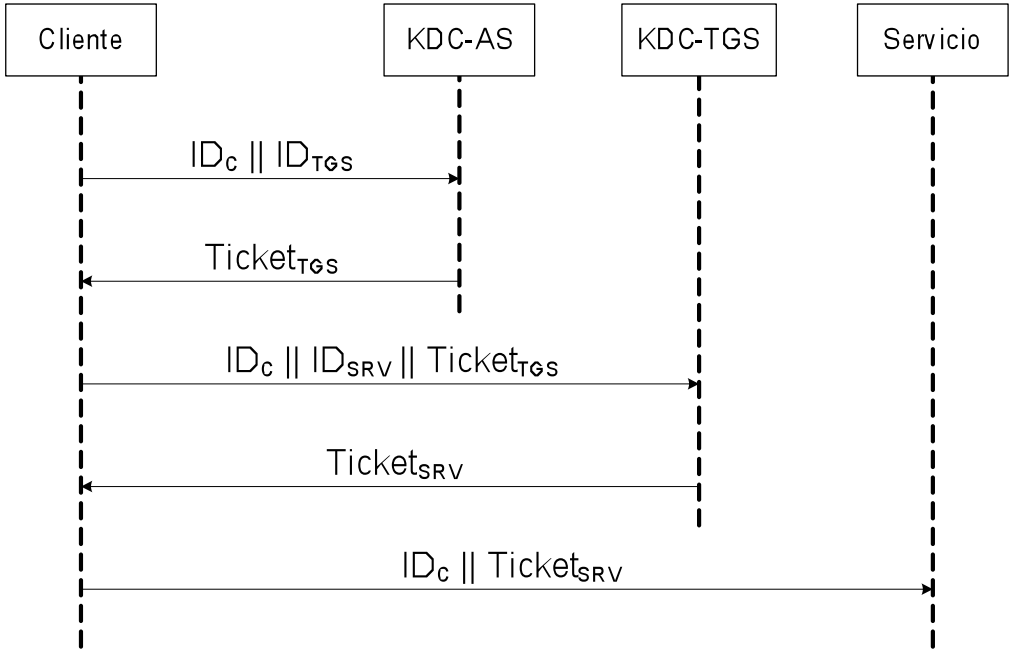
- Login basado en clave
  - Una clave por servicio/sesión
- Login empleando una base de datos única



  - Problemas de operativa
    - Un login por sesión
    - Clave circula en claro

Construcción del protocolo

- Login basado en tickets de acceso



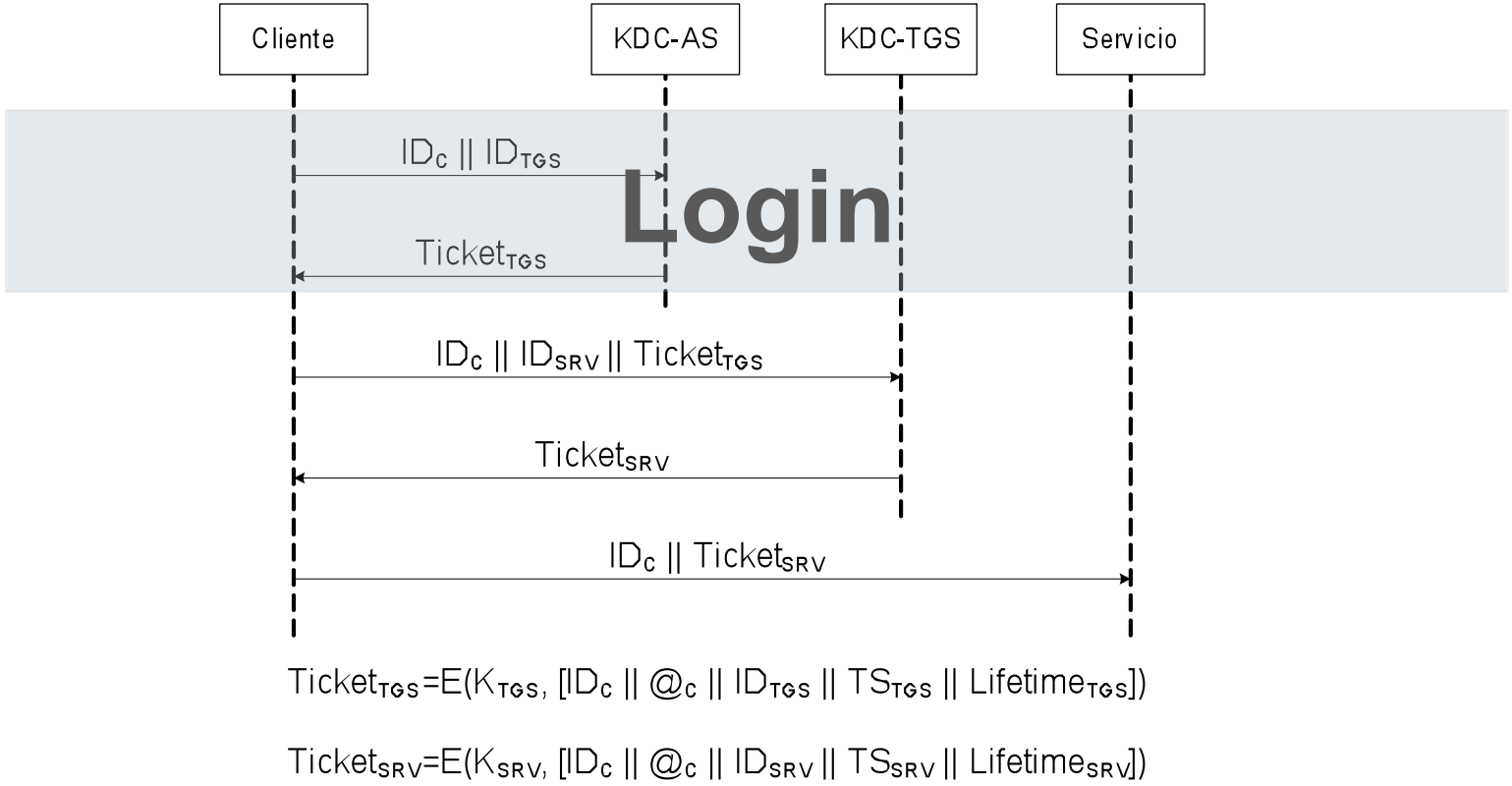
$Ticket_{TGS}=E(K_{TGS}, [ID_C \| @_C \| ID_{TGS} \| TS_{TGS} \| Lifetime_{TGS}])$

$Ticket_{SRV}=E(K_{SRV}, [ID_C \| @_C \| ID_{SRV} \| TS_{SRV} \| Lifetime_{SRV}])$

- Problemas de operativa
  - Validez temporal del ticket
  - Autenticación mutua
  - Replicación de dirección

Construcción del protocolo

- Login basado en tickets de acceso



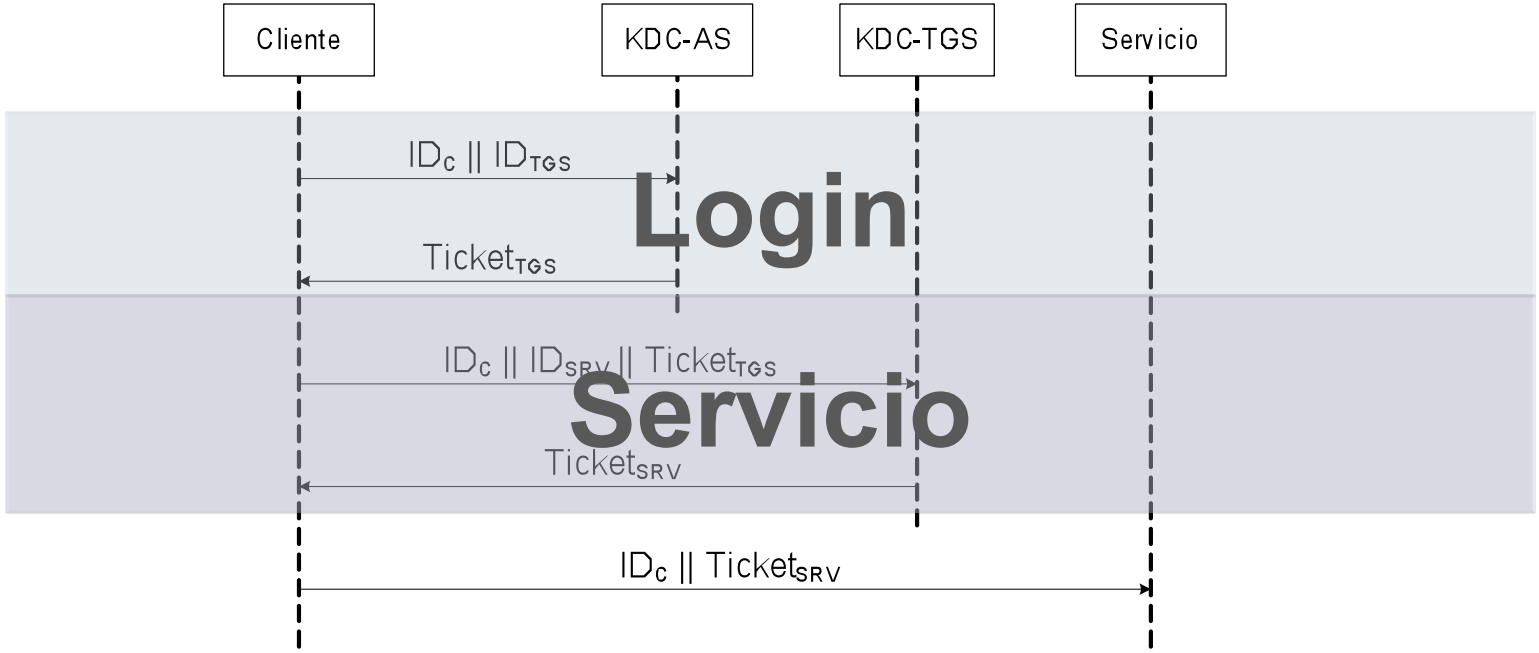
$Ticket_{TGS}=E(K_{TGS}, [ID_C \| @_C \| ID_{TGS} \| TS_{TGS} \| Lifetime_{TGS}])$

$Ticket_{SRV}=E(K_{SRV}, [ID_C \| @_C \| ID_{SRV} \| TS_{SRV} \| Lifetime_{SRV}])$

- Problemas de operativa
  - Validez temporal del ticket
  - Autenticación mutua
  - Replicación de dirección

Construcción del protocolo

- Login basado en tickets de acceso



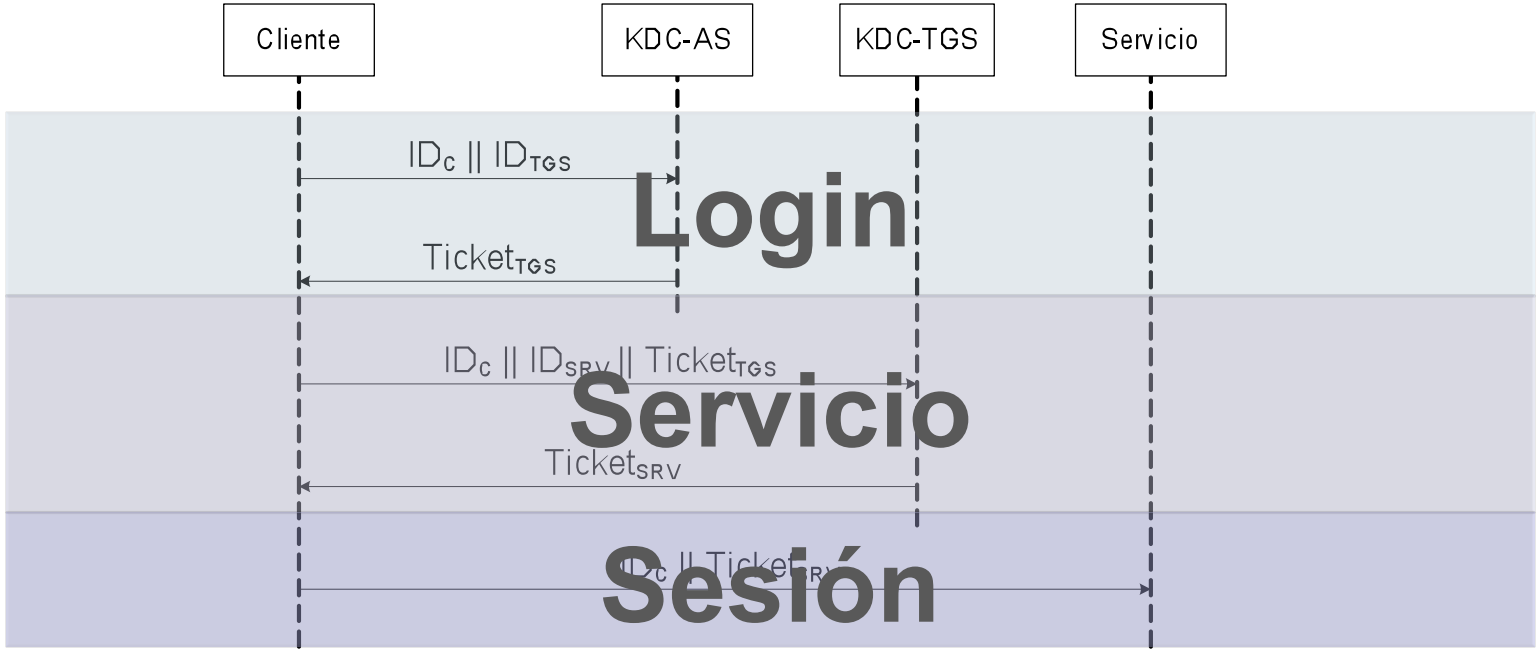
$Ticket_{TGS}=E(K_{TGS}, [ID_C \| @_C \| ID_{TGS} \| TS_{TGS} \| Lifetime_{TGS}])$

$Ticket_{SRV}=E(K_{SRV}, [ID_C \| @_C \| ID_{SRV} \| TS_{SRV} \| Lifetime_{SRV}])$

- Problemas de operativa
  - Validez temporal del ticket
  - Autenticación mutua
  - Replicación de dirección

Construcción del protocolo

- Login basado en tickets de acceso



$Ticket_{TGS}=E(K_{TGS}, [ID_C \| @_C \| ID_{TGS} \| TS_{TGS} \| Lifetime_{TGS}])$

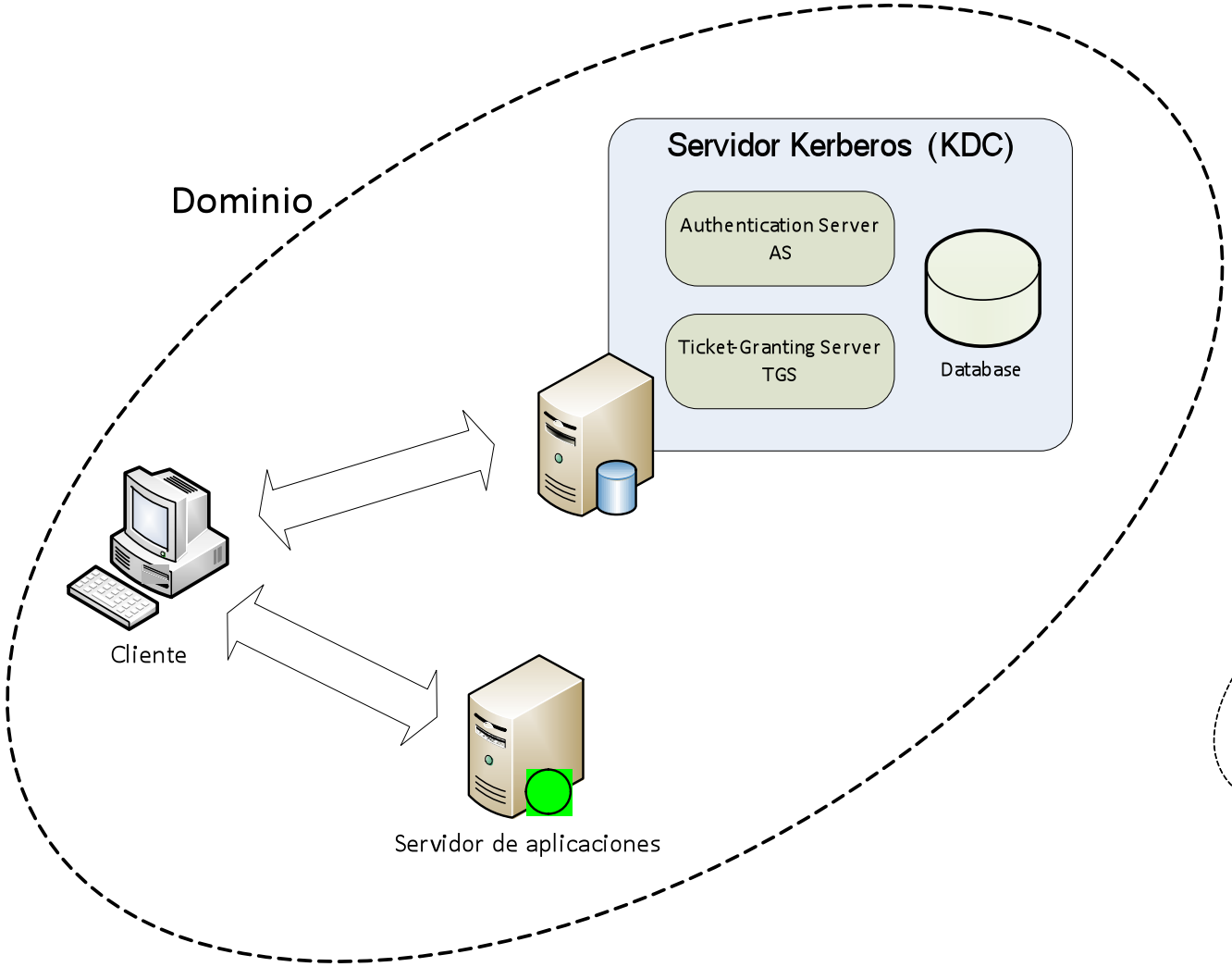
$Ticket_{SRV}=E(K_{SRV}, [ID_C \| @_C \| ID_{SRV} \| TS_{SRV} \| Lifetime_{SRV}])$

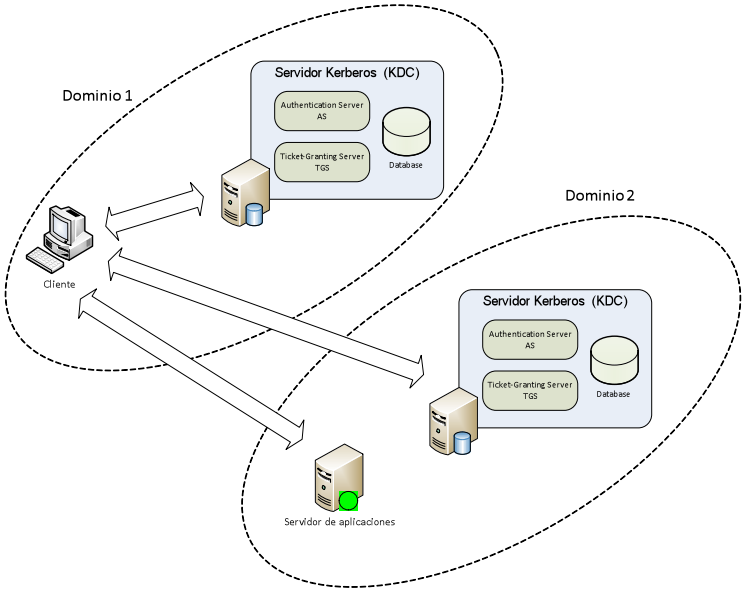
- Problemas de operativa
  - Validez temporal del ticket
  - Autenticación mutua
  - Replicación de dirección

Estructura

- Cliente
- Servidor de autenticación (AS, *Authentication Server*)
  - Responde a petición de autenticación inicial del usuario no autenticado.
  - Genera Ticket Granting Ticket (TGT) para petición de acceso a servicios.
- Servidor de tickets de servicio (TGS, *Ticket-Granting Service*)
  - Distribuye tickets de servicio a partir de un TGT válido
- Base de datos (*Database*)
  - Contenedor de las entradas asociadas a los usuarios y servicios.
  - Indexadas por *principal* (nombre@dominio) de usuario o servicio
- Servidor de aplicaciones y servicios
- Dominio (*Realm*)
  - Entorno administrativo de autenticación

Estructura


Dominio
Servidor Kerberos (KDC)
Authentication Server AS
Ticket-Granting Server TGS
Database
Cliente
Servidor de aplicaciones


Dominio 1
Servidor Kerberos (KDC)
Authentication Server AS
Ticket-Granting Server TGS
Database
Cliente
Dominio 2
Servidor Kerberos (KDC)
Authentication Server AS
Ticket-Granting Server TGS
Database
Servidor de aplicaciones

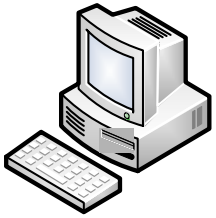
Terminología

- Ticket
  - Token empleado por el usuario que permite transferir de forma segura su identidad. Es un prueba de autenticidad de la identidad.
  - Contiene la información necesaria establecer una comunicación segura entre el cliente y los servidores (claves, identidad, etc.).
  - No puede ser modificada por el cliente ya que se cifra con la clave del servidor al que está dirigido.
  - Puede tener asociada una validez temporal limitada.
- Clave de sesión (*Session key*)
  - Clave temporal con la que cifrar y autenticar la comunicación entre el usuario y el servicio
- Autenticador (*Authenticator*)
  - Token generado por el cliente y de un solo uso que prueba la identidad y la actualidad de la información para acceder a un servicio.
  - Cifrado con clave de sesión entre entidades (incluida en el ticket).

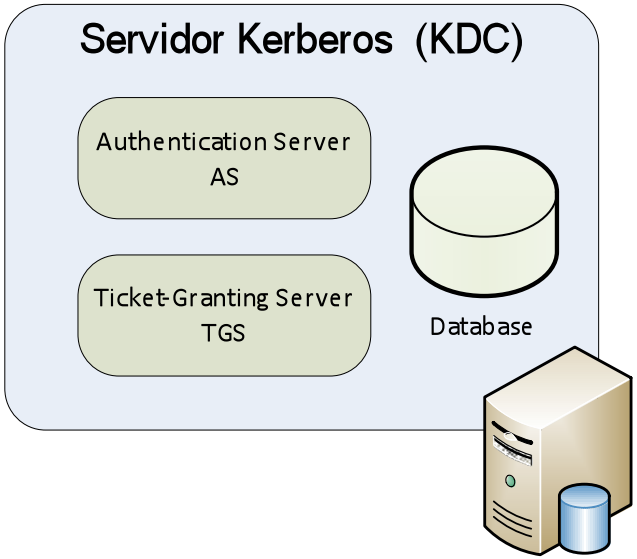
Terminología

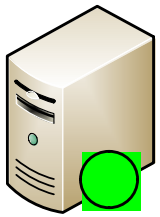
- Validez temporal (*Lifetime*)
  - Periodo de tiempo que el ticket o token es válido
- Sello de tiempo (*Timestamp*)
  - Momento en el que se ha creado el elemento
- Número aleatorio (*Nonce*)
  - Dato para prevenir ataques por repetición

Protocolo (versión 4)



Cliente

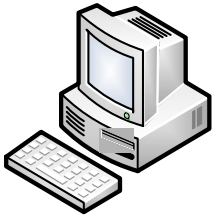




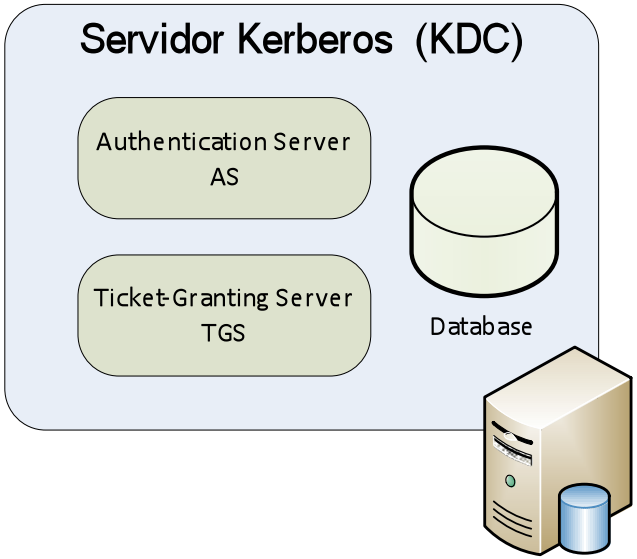
Servidor de aplicaciones

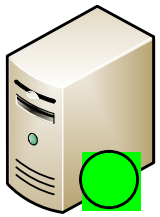
Protocolo (versión 4)

Usuario desea acceder a un servicio



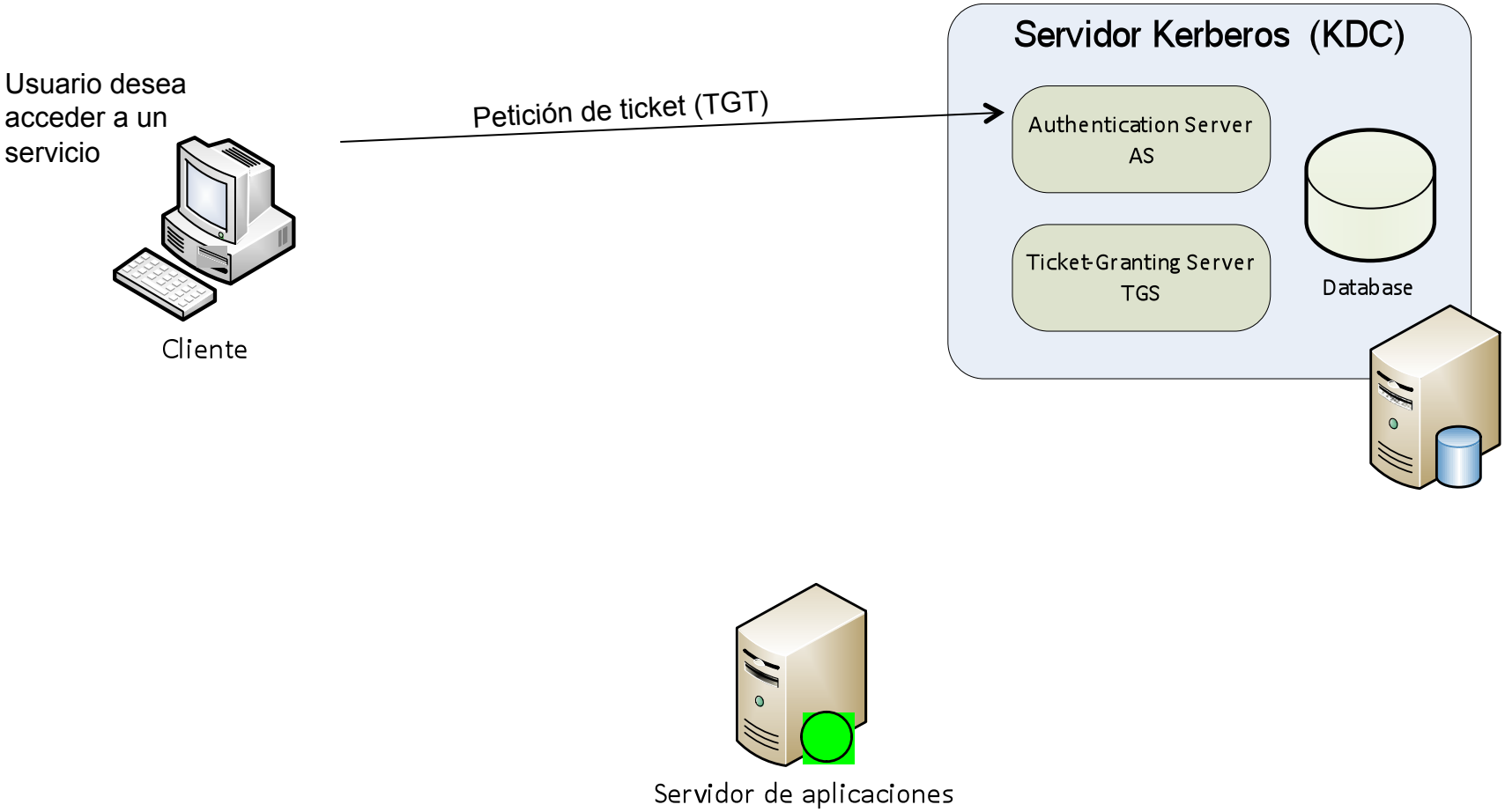
Cliente



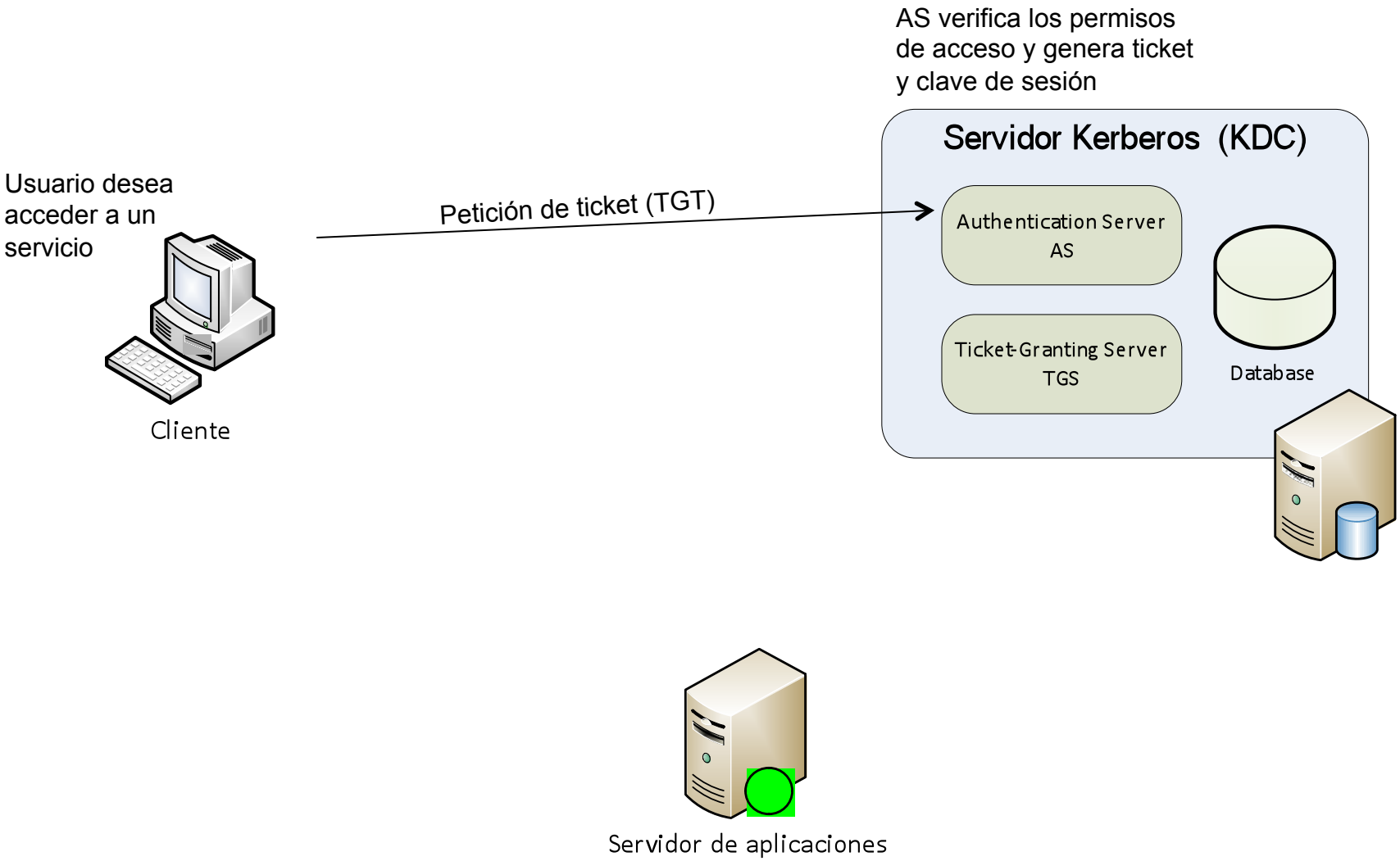


Servidor de aplicaciones

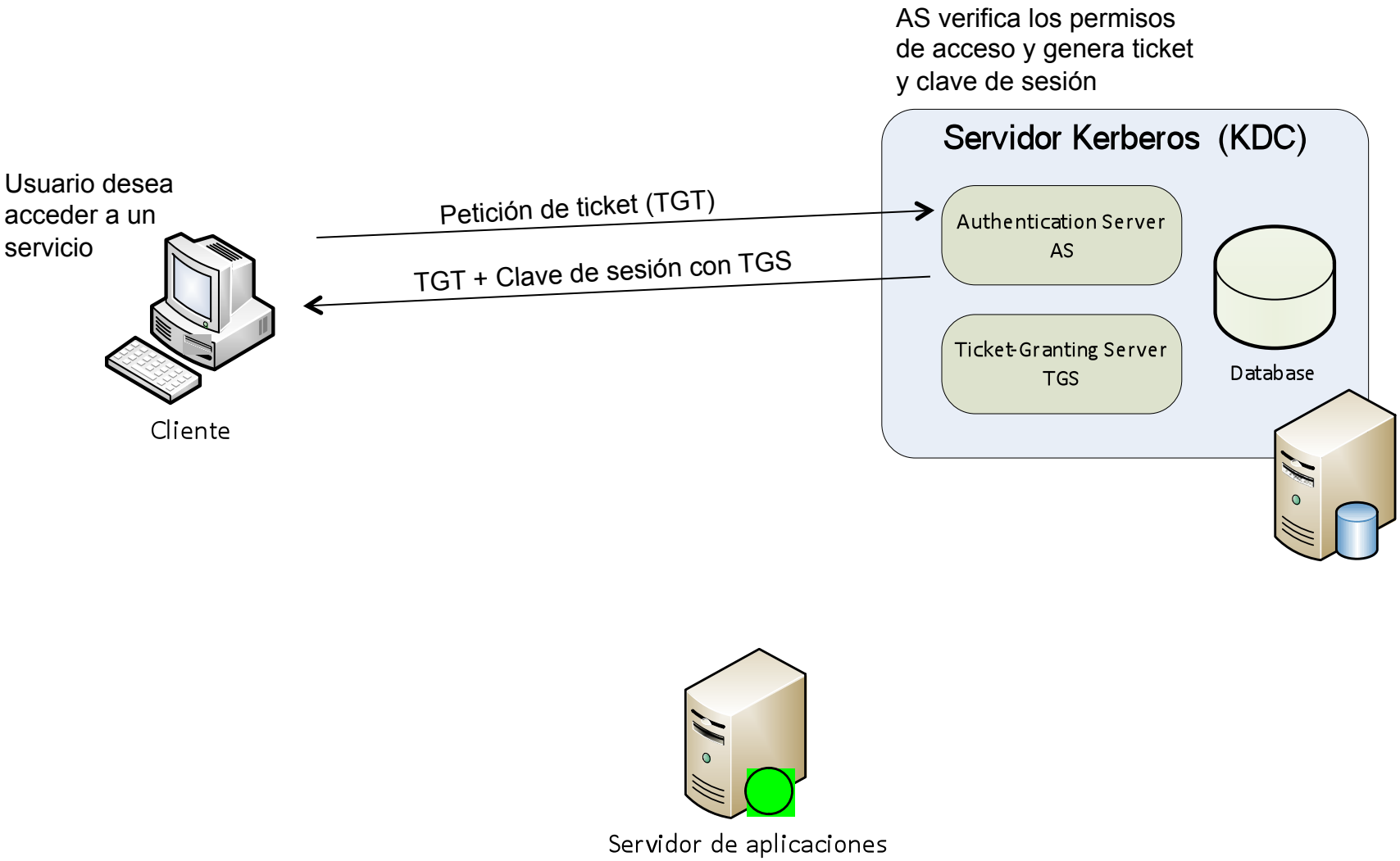
Protocolo (versión 4)



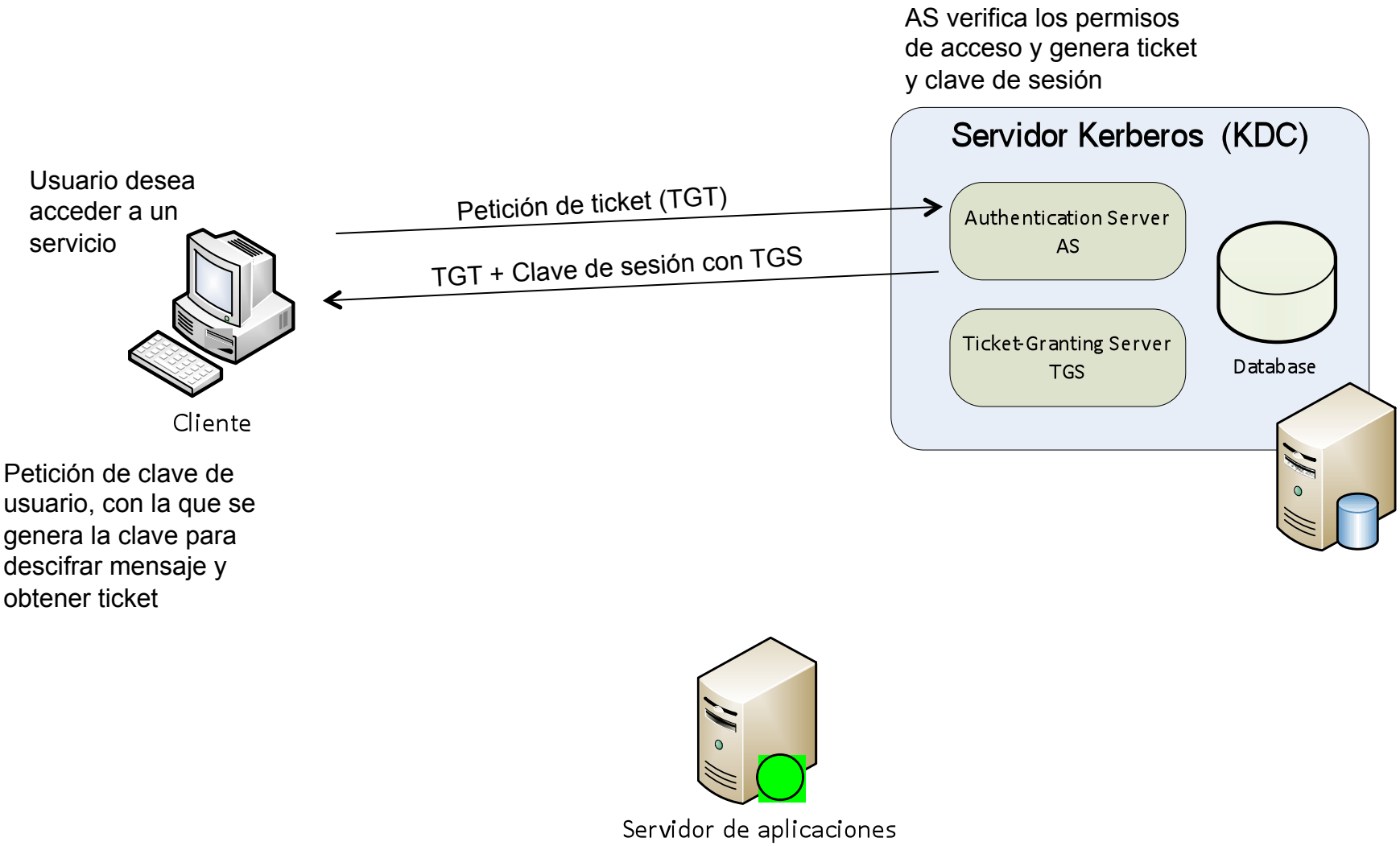
Protocolo (versión 4)



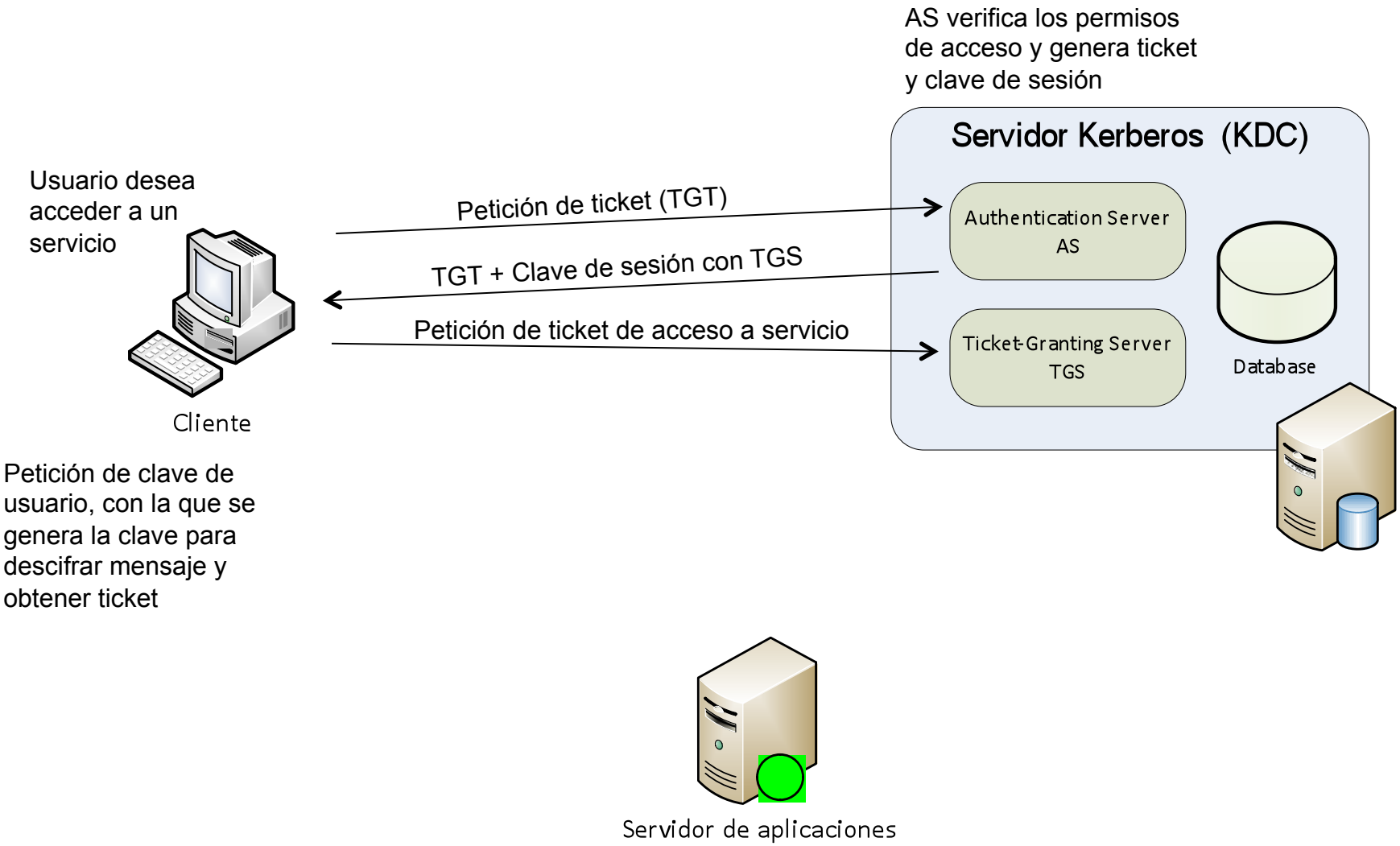
Protocolo (versión 4)



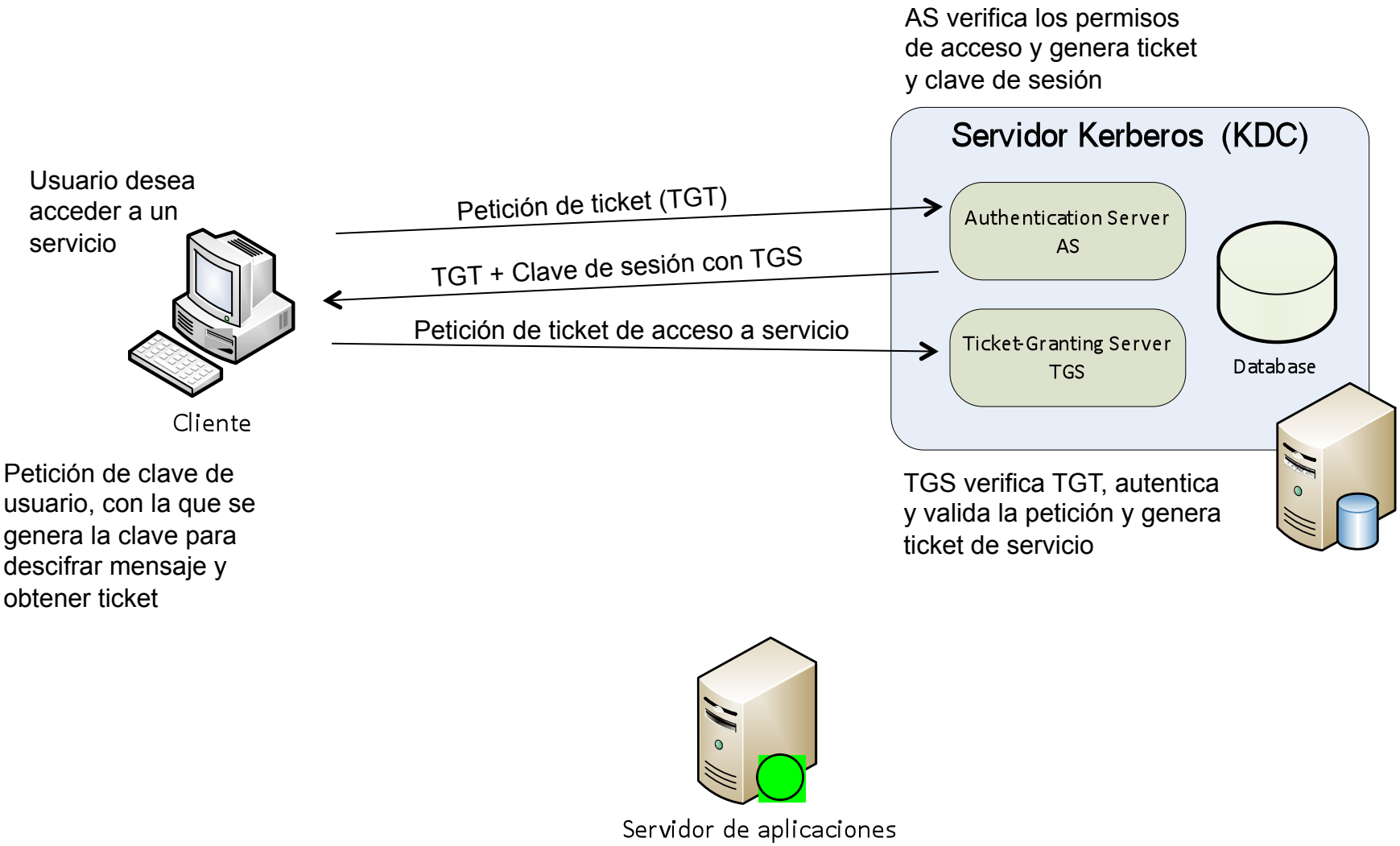
Protocolo (versión 4)



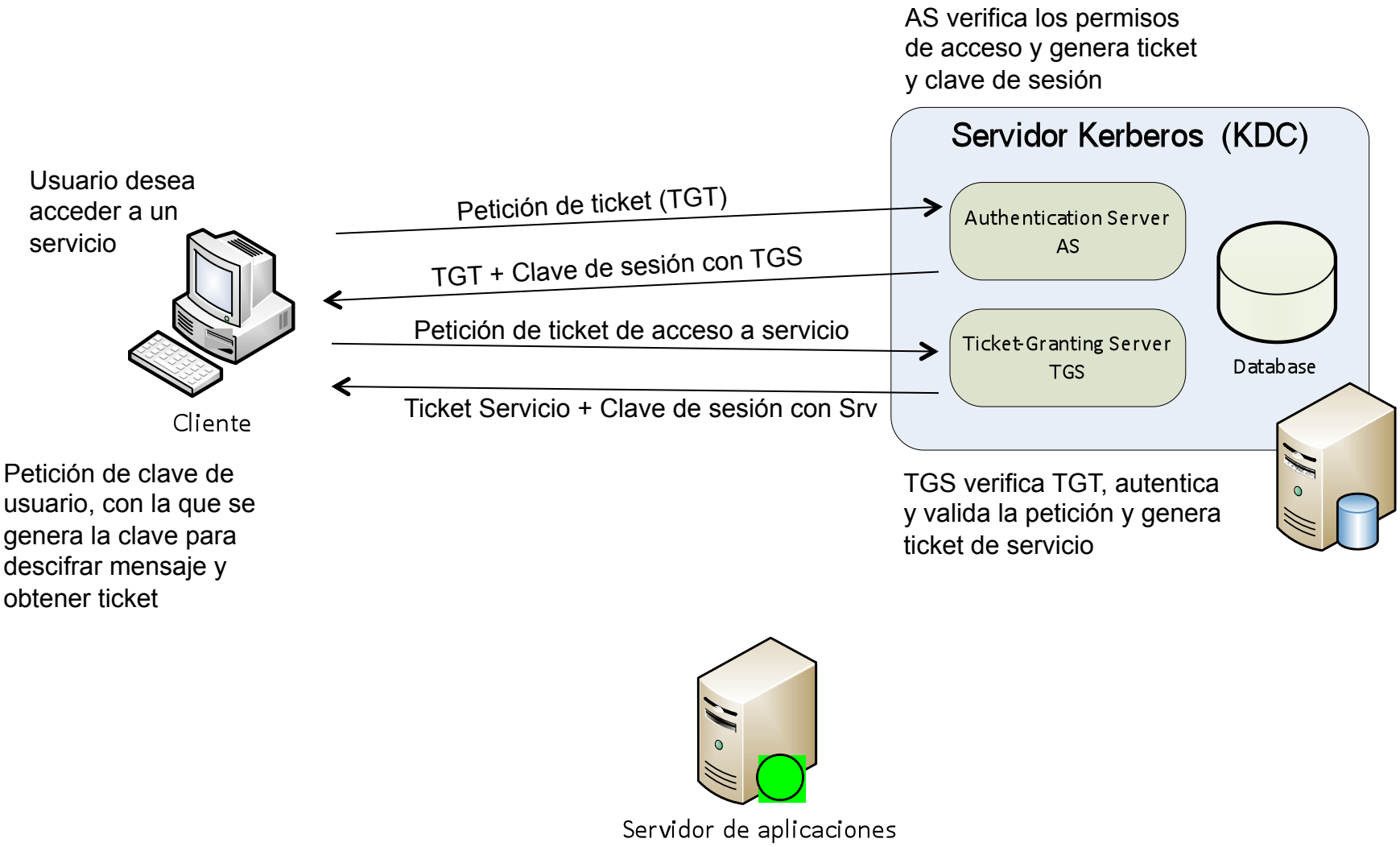
Protocolo (versión 4)



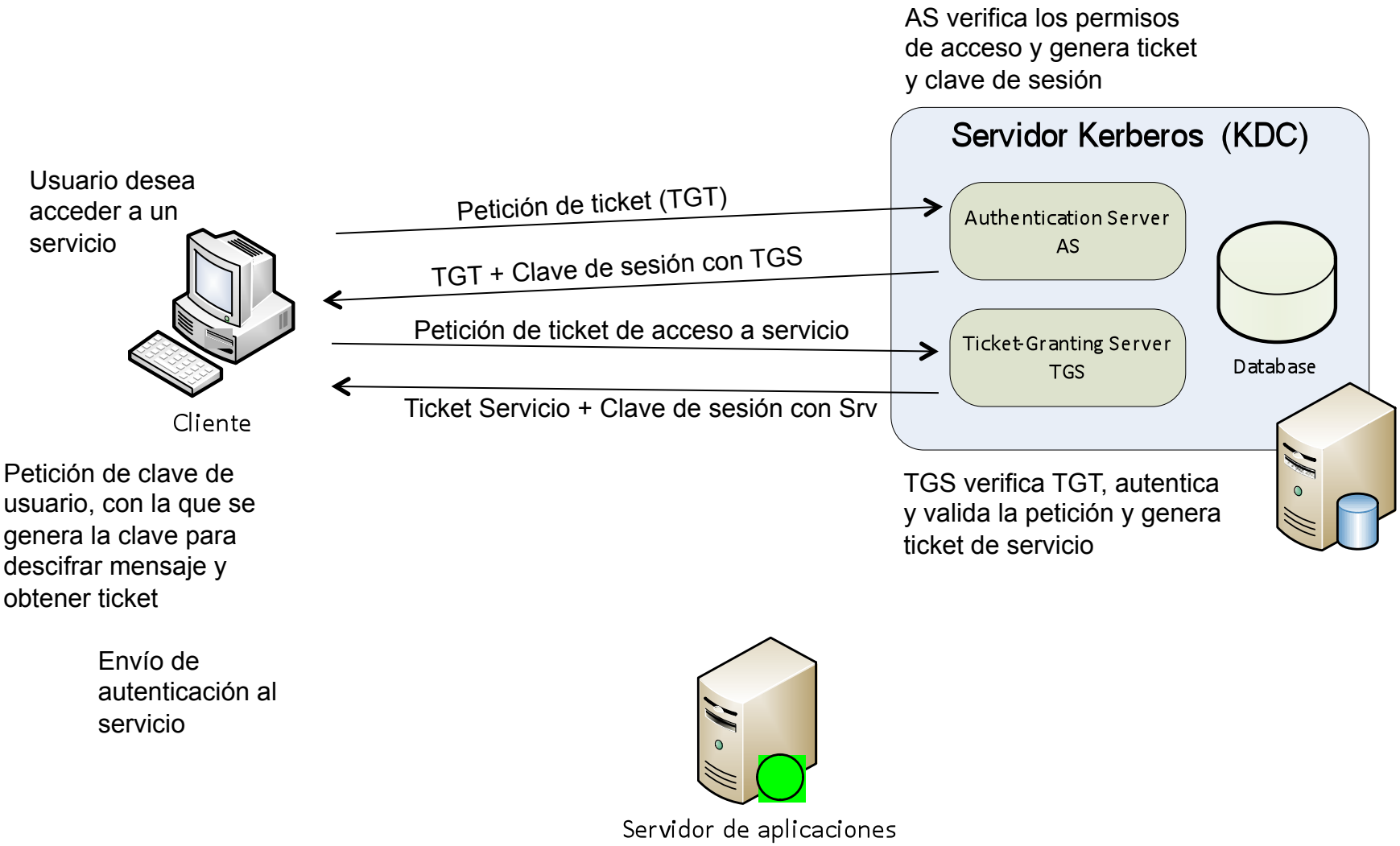
Protocolo (versión 4)



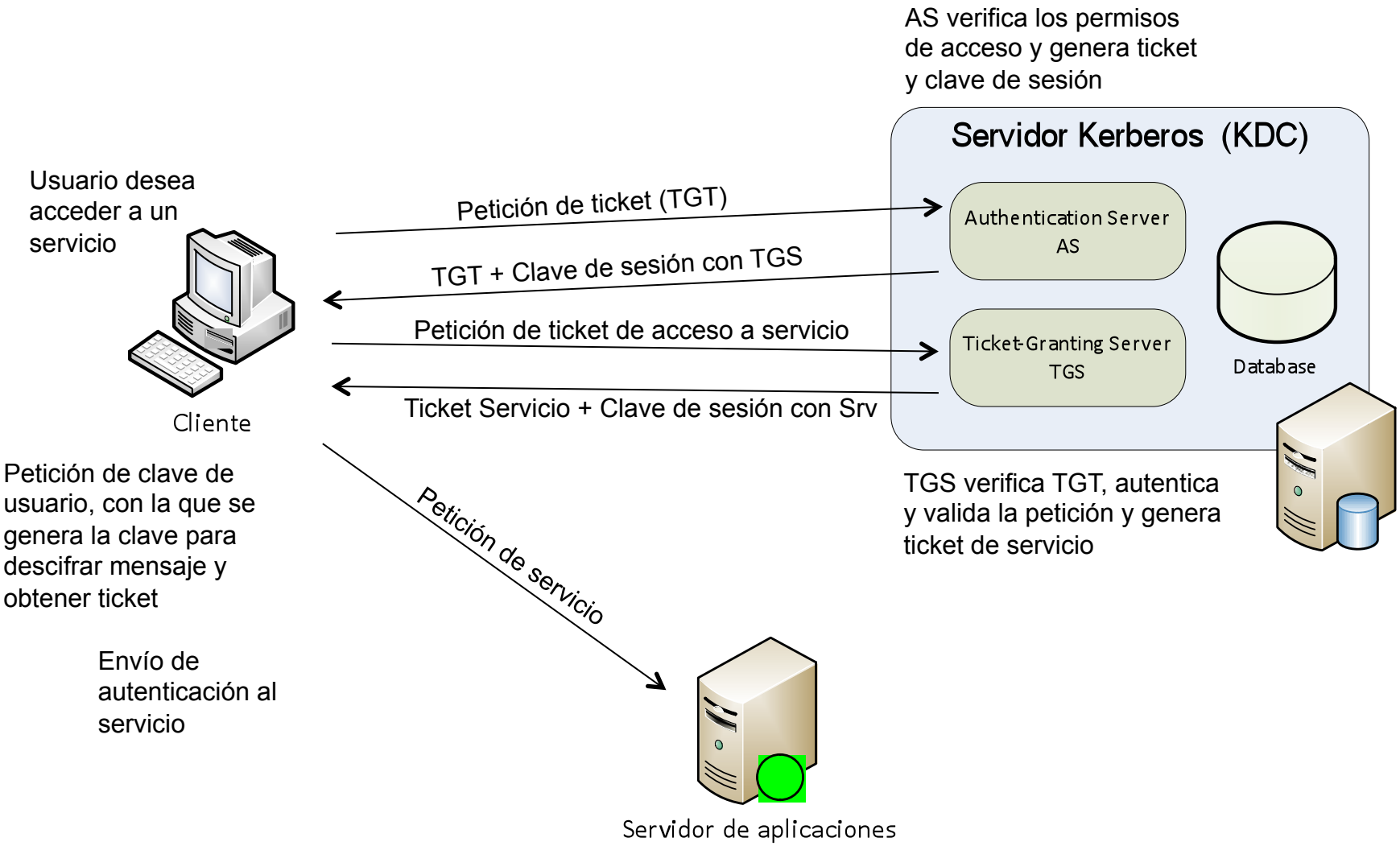
Protocolo (versión 4)



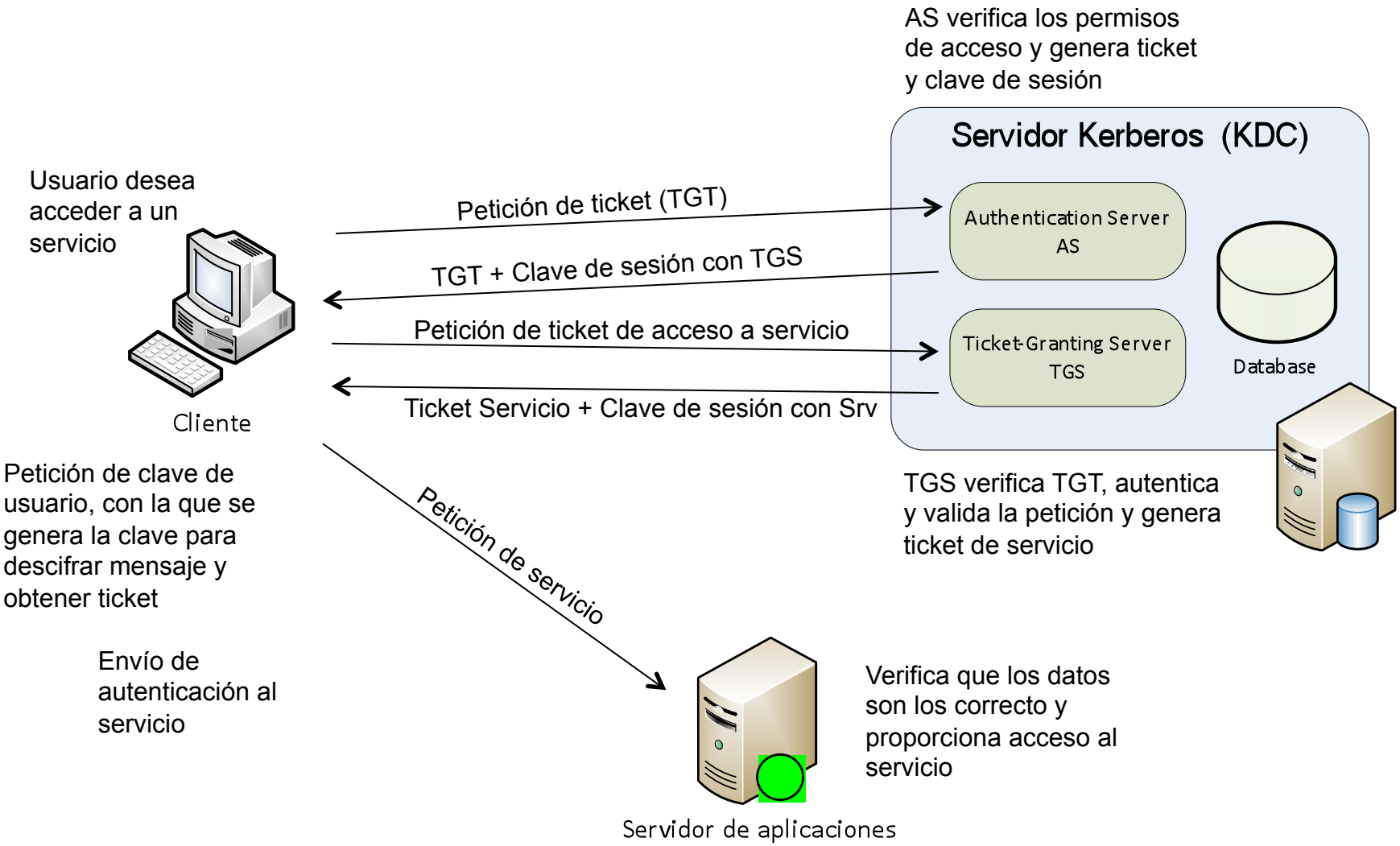
Protocolo (versión 4)



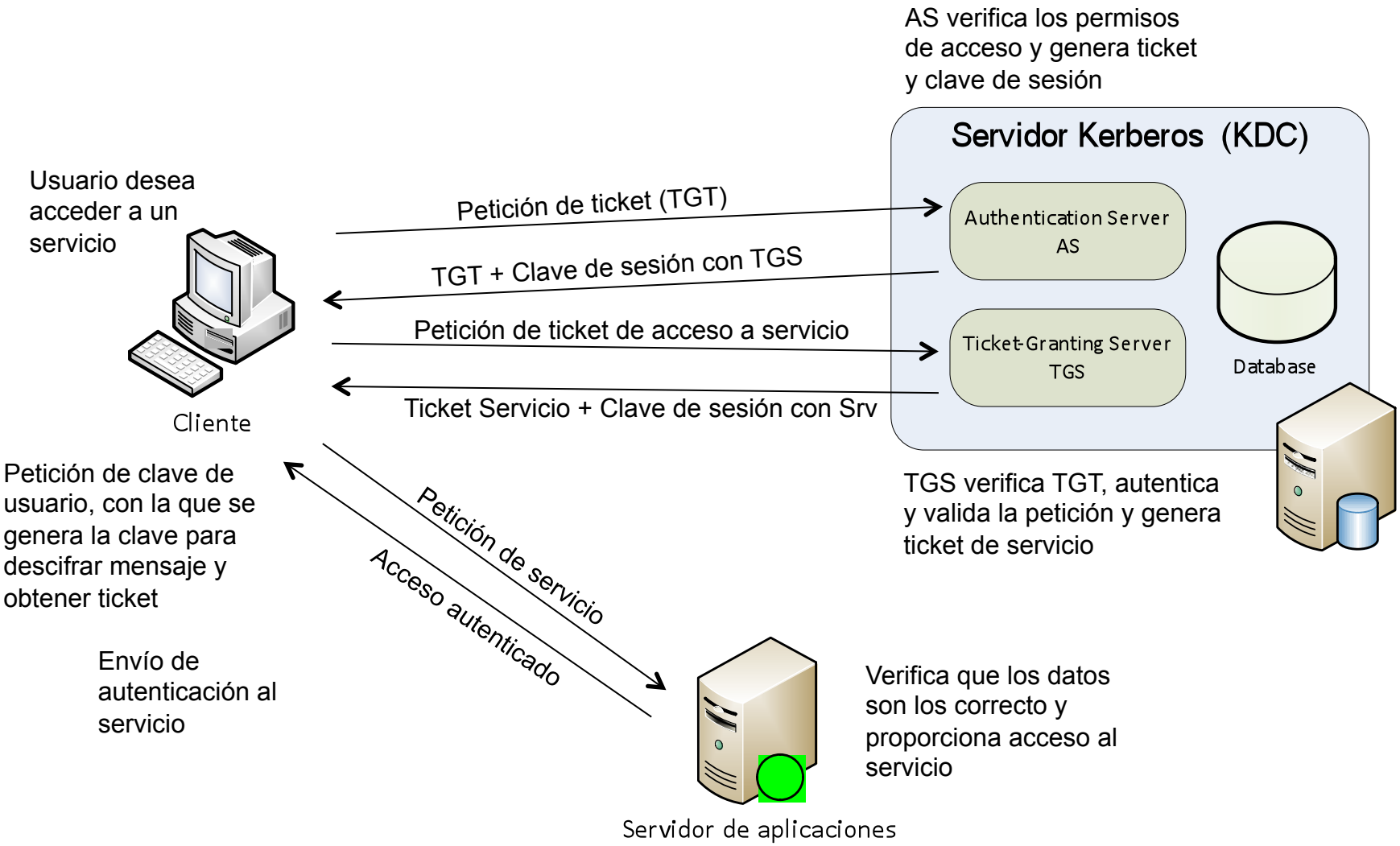
Protocolo (versión 4)



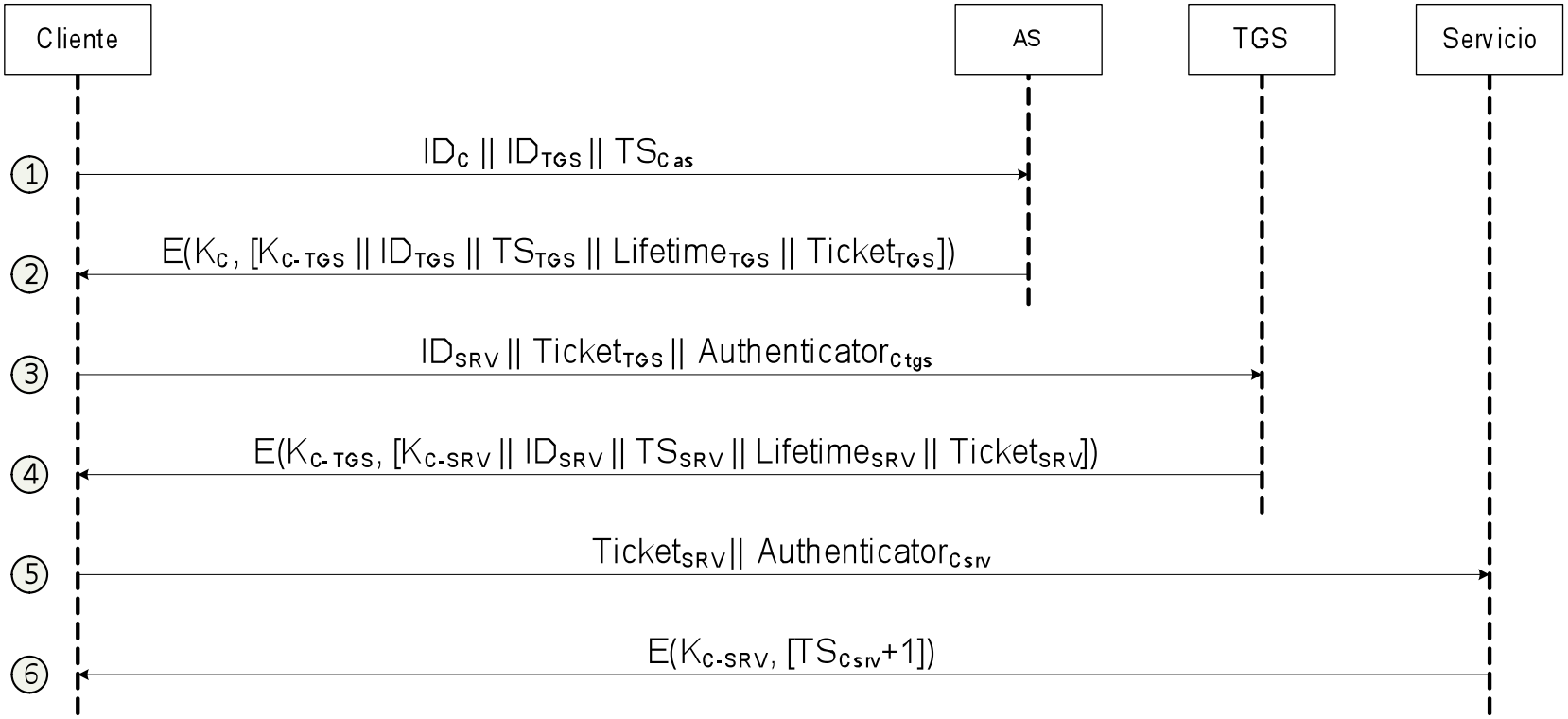
Protocolo (versión 4)



Protocolo (versión 4)



Protocolo (versión 4)



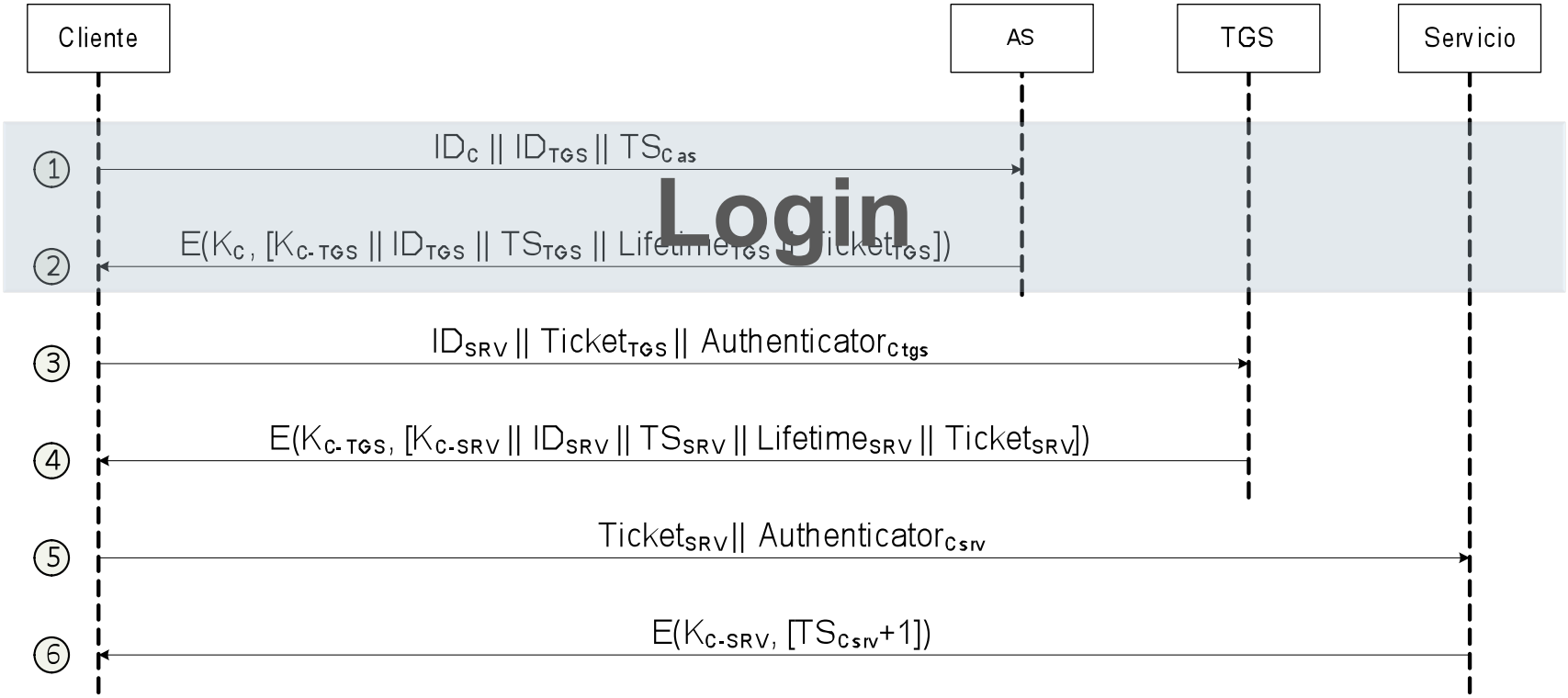
$Ticket_{TGS}=E(K_{TGS}, [K_{C\text{-}TGS} \| ID_C \| @C \| ID_{TGS} \| TS_{TGS} \| Lifetime_{TGS}])$

$Authenticator_{Ctgs}=E(K_{C\text{-}TGS}, [ID_C \| @C \| TS_{Ctgs}])$

$Ticket_{SRV}=E(K_{SRV}, [K_{C\text{-}TGS} \| ID_C \| @C \| ID_{SRV} \| TS_{SRV} \| Lifetime_{SRV}])$

$Authenticator_{SRV}=E(K_{C\text{-}SRV}, [ID_C \| @C \| TS_{Csrv}])$

Protocolo (versión 4)



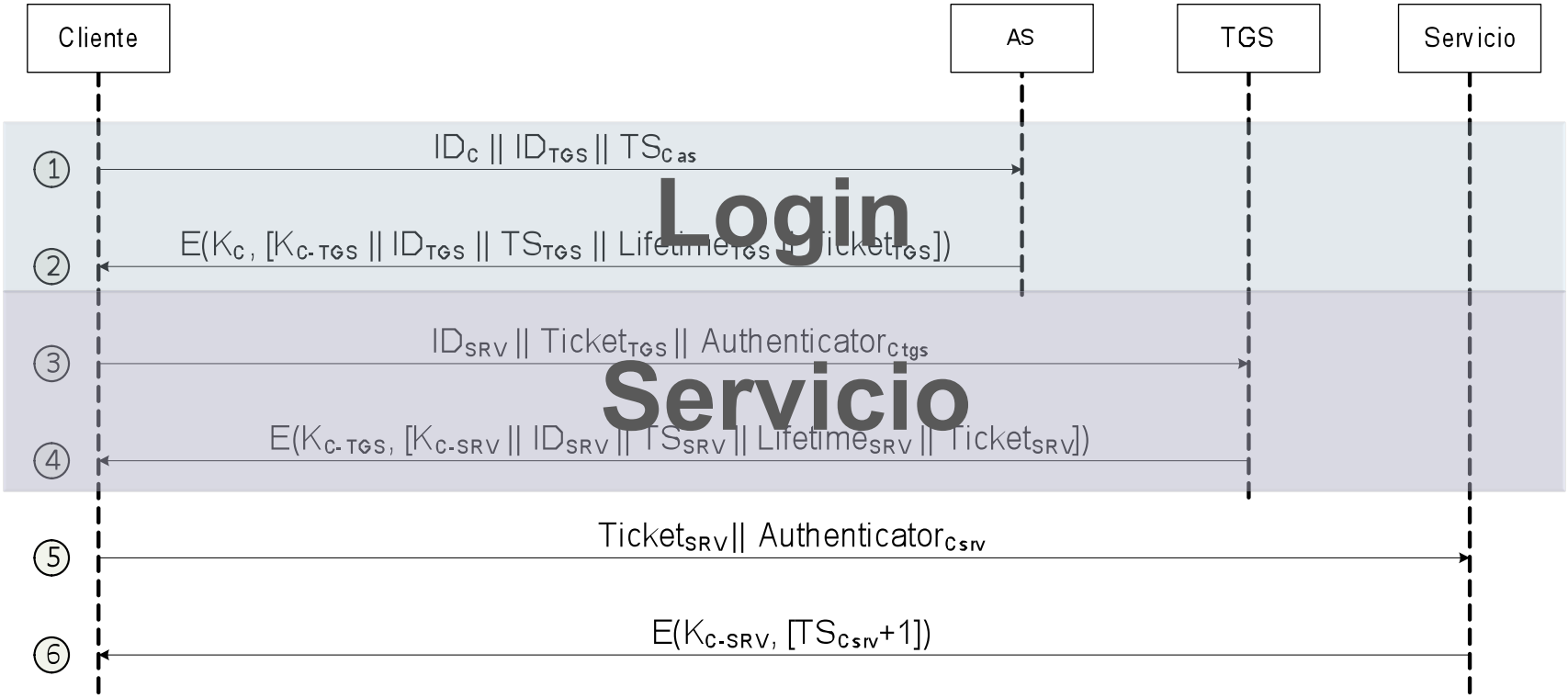
$Ticket_{TGS}=E(K_{TGS}, [K_{C\text{-}TGS} \| ID_C \| @C \| ID_{TGS} \| TS_{TGS} \| Lifetime_{TGS}])$

$Authenticator_{Ctgs}=E(K_{C\text{-}TGS}, [ID_C \| @C \| TS_{Ctgs}])$

$Ticket_{SRV}=E(K_{SRV}, [K_{C\text{-}TGS} \| ID_C \| @C \| ID_{SRV} \| TS_{SRV} \| Lifetime_{SRV}])$

$Authenticator_{SRV}=E(K_{C\text{-}SRV}, [ID_C \| @C \| TS_{Csrv}])$

Protocolo (versión 4)



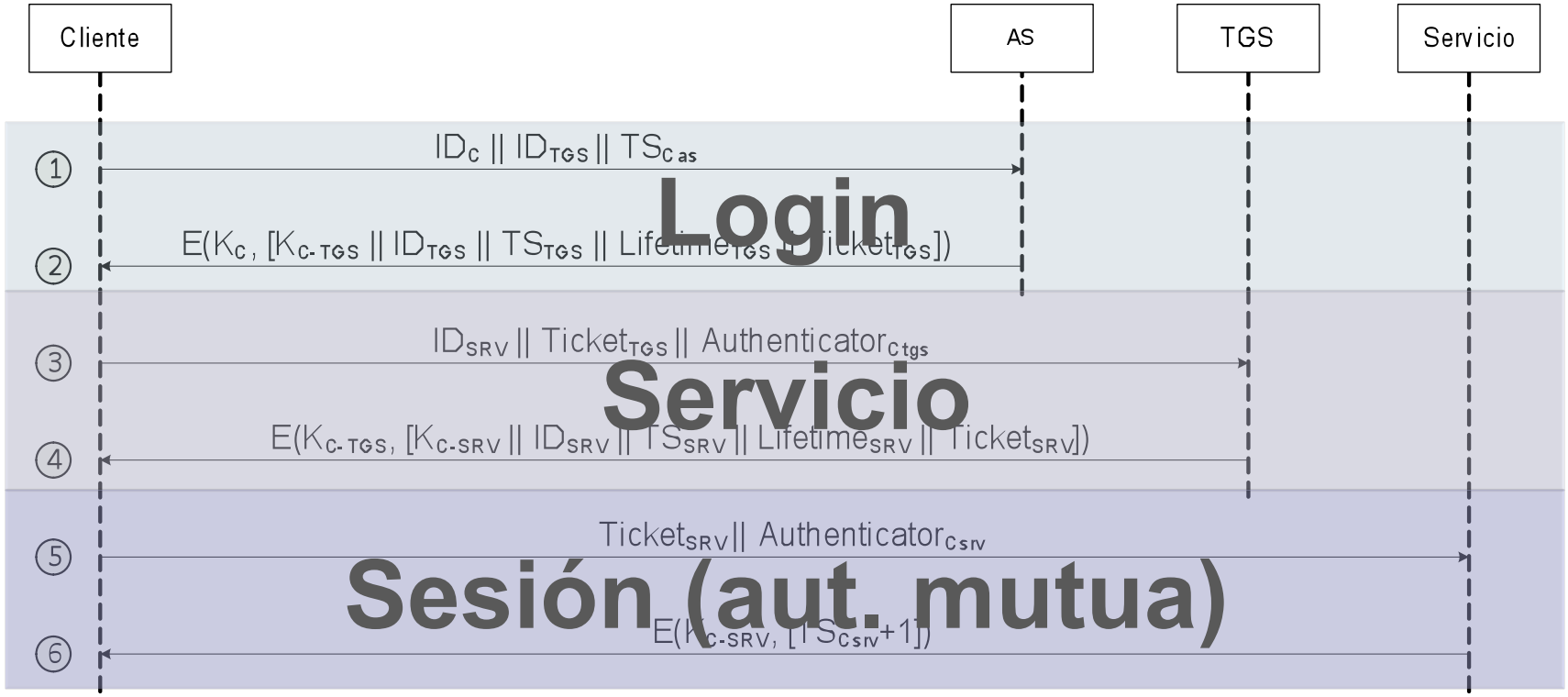
$Ticket_{TGS}=E(K_{TGS}, [K_{C\text{-}TGS} \| ID_C \| @C \| ID_{TGS} \| TS_{TGS} \| Lifetime_{TGS}])$

$Authenticator_{Ctgs}=E(K_{C\text{-}TGS}, [ID_C \| @C \| TS_{Ctgs}])$

$Ticket_{SRV}=E(K_{SRV}, [K_{C\text{-}TGS} \| ID_C \| @C \| ID_{SRV} \| TS_{SRV} \| Lifetime_{SRV}])$

$Authenticator_{SRV}=E(K_{C\text{-}SRV}, [ID_C \| @C \| TS_{Csrv}])$

Protocolo (versión 4)



$Ticket_{TGS}=E(K_{TGS}, [K_{C\text{-}TGS} \| ID_C \| @C \| ID_{TGS} \| TS_{TGS} \| Lifetime_{TGS}])$

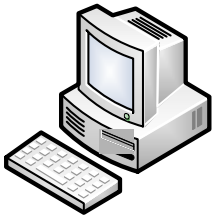
$Authenticator_{Ctgs}=E(K_{C\text{-}TGS}, [ID_C \| @C \| TS_{Ctgs}])$

$Ticket_{SRV}=E(K_{SRV}, [K_{C\text{-}TGS} \| ID_C \| @C \| ID_{SRV} \| TS_{SRV} \| Lifetime_{SRV}])$

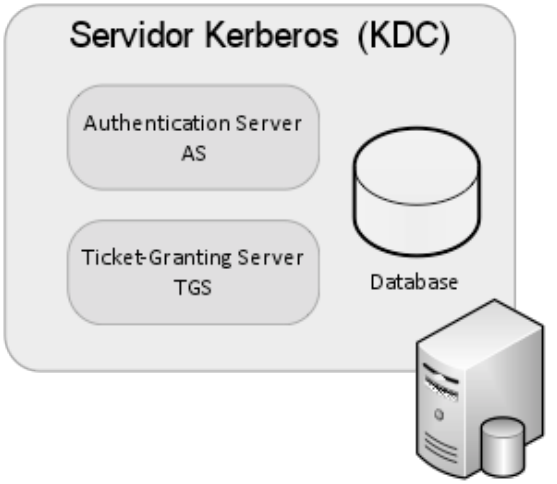
$Authenticator_{SRV}=E(K_{C\text{-}SRV}, [ID_C \| @C \| TS_{Csrv}])$

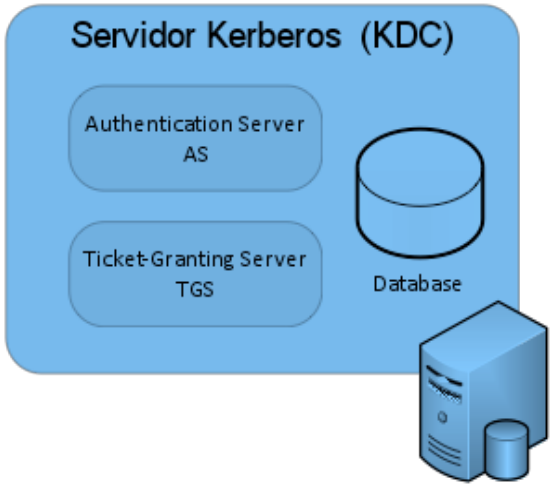
Protocolo versión 4

- Soporte multi-dominio



Cliente

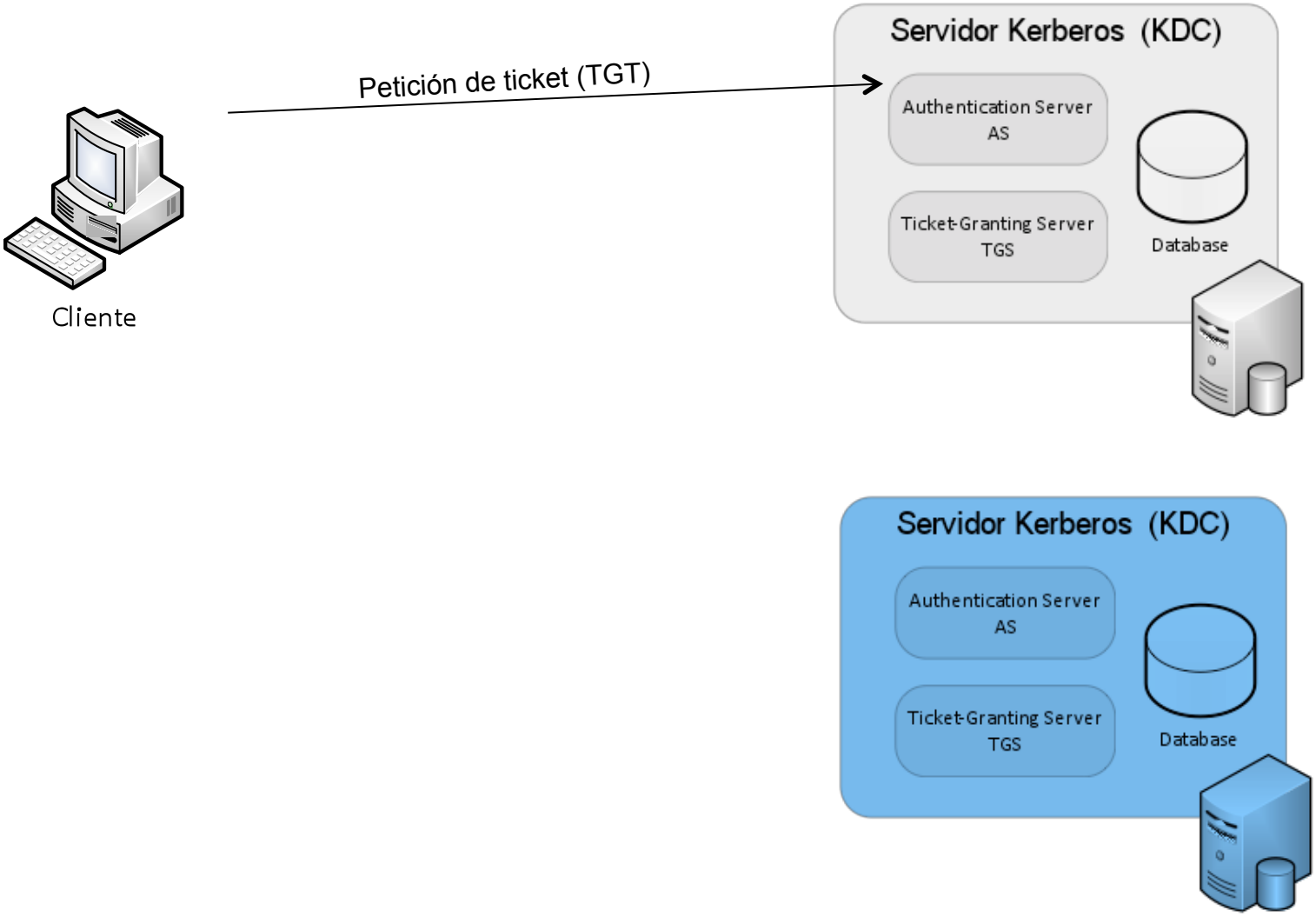




Servidor de aplicaciones

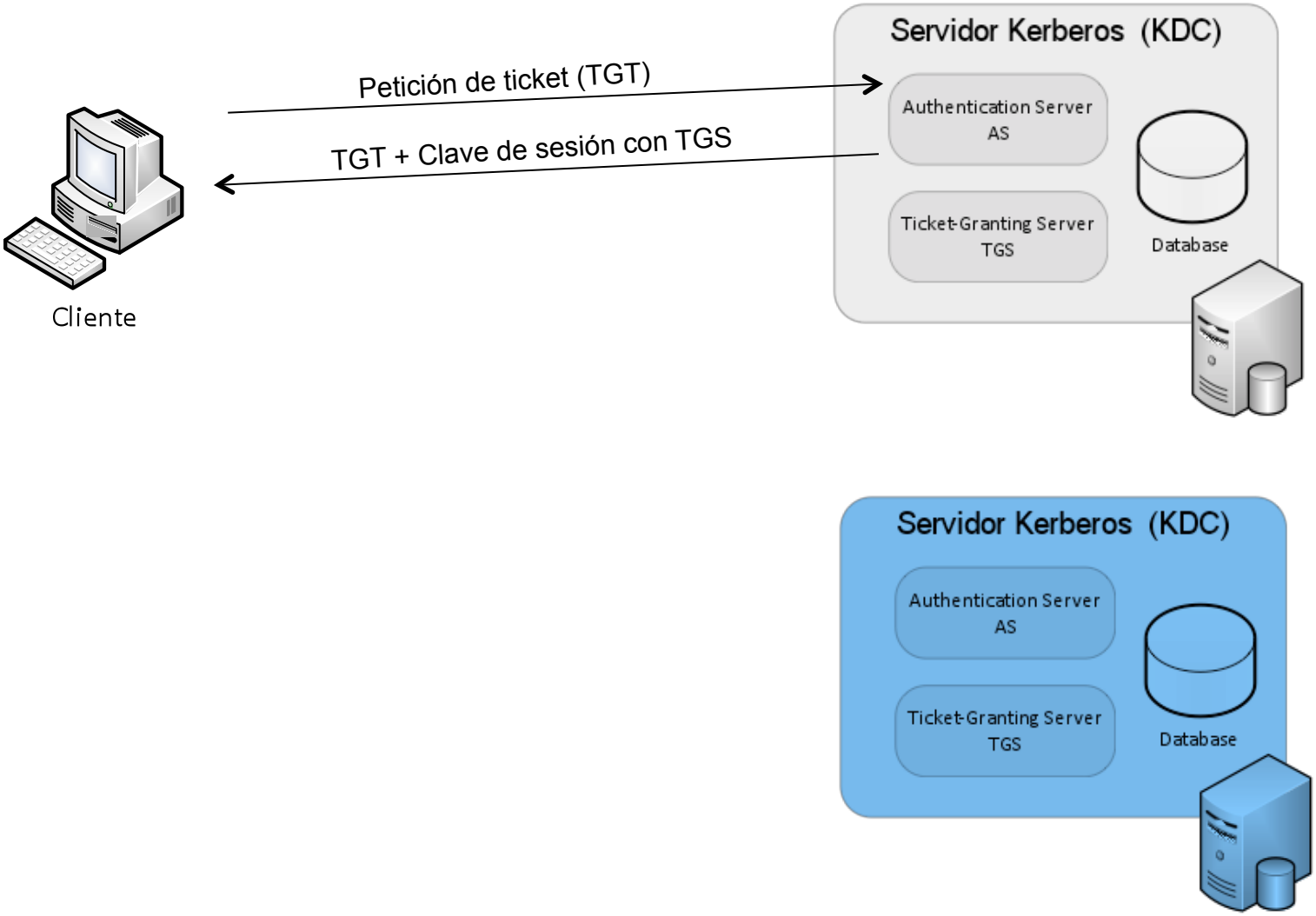
Protocolo versión 4

- Soporte multi-dominio



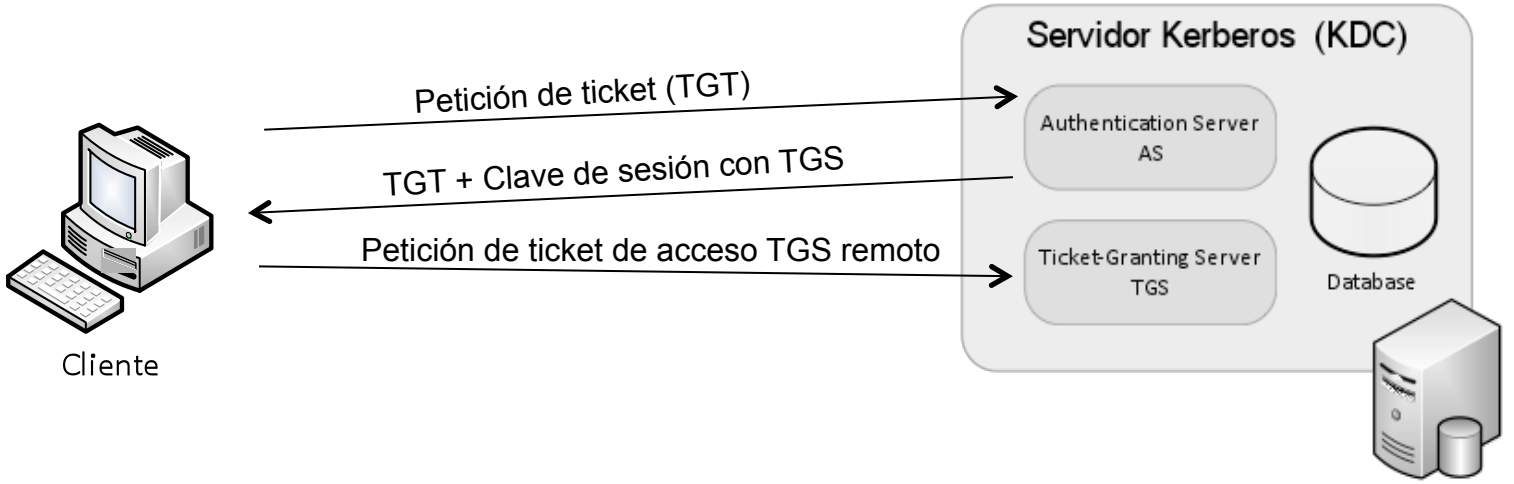
Protocolo versión 4

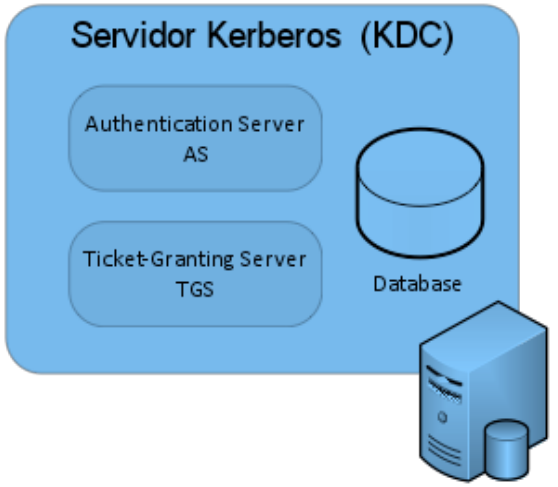
- Soporte multi-dominio



Protocolo versión 4

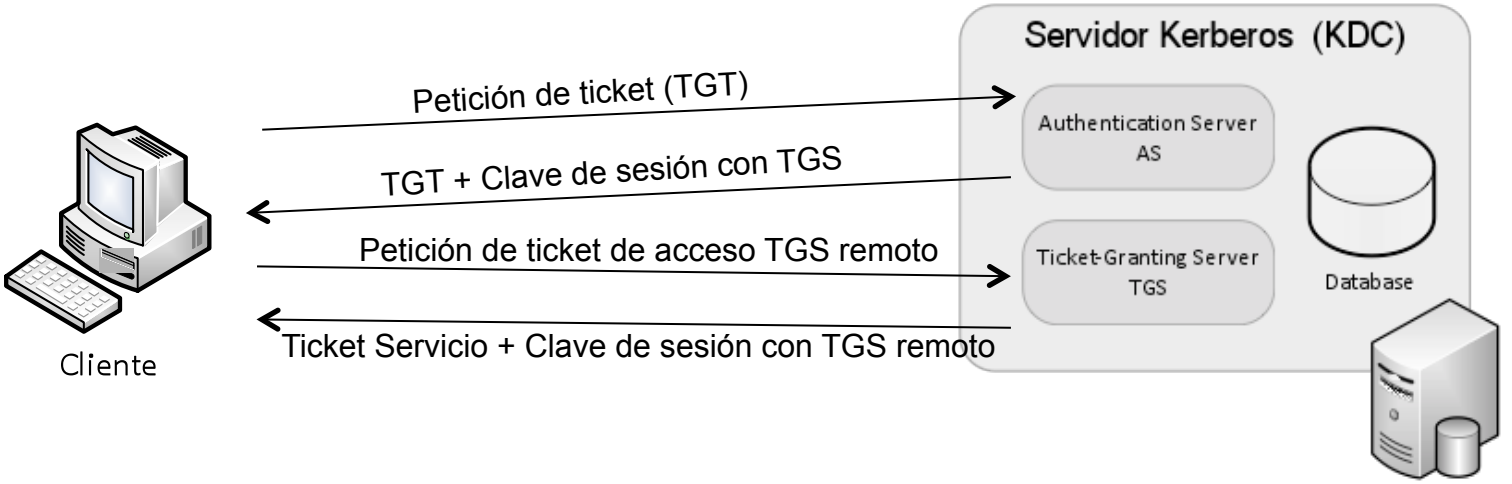
- Soporte multi-dominio

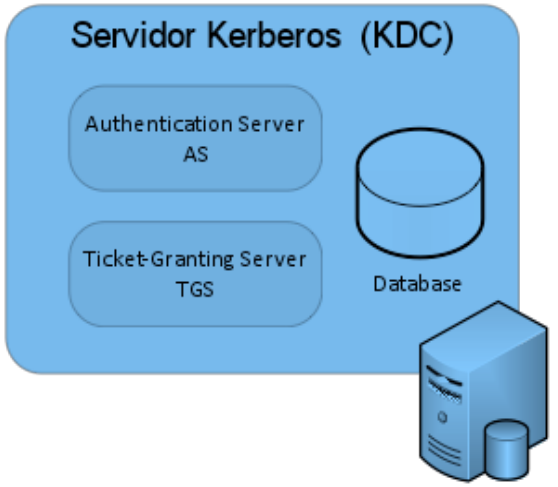




Protocolo versión 4

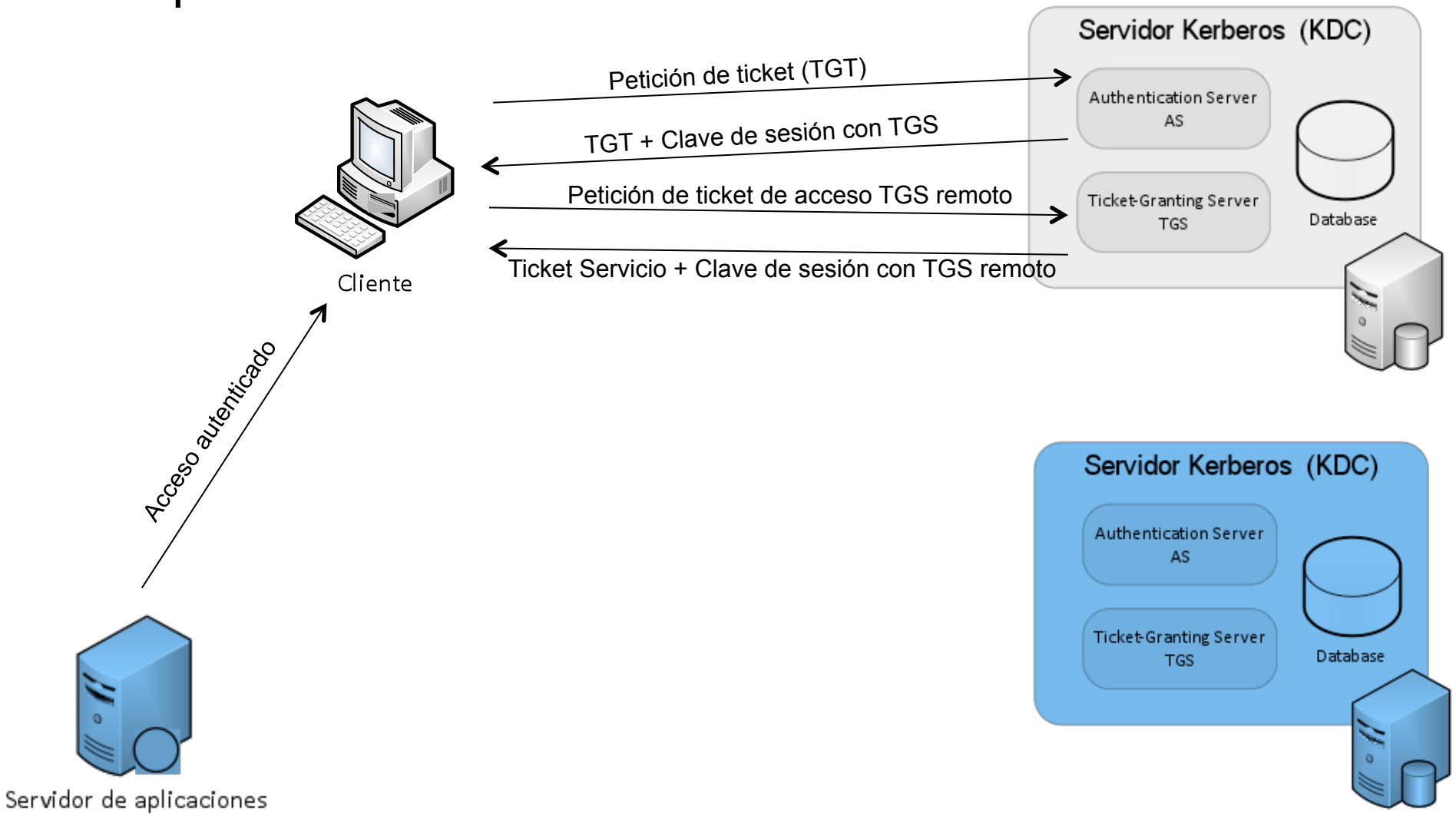
- Soporte multi-dominio





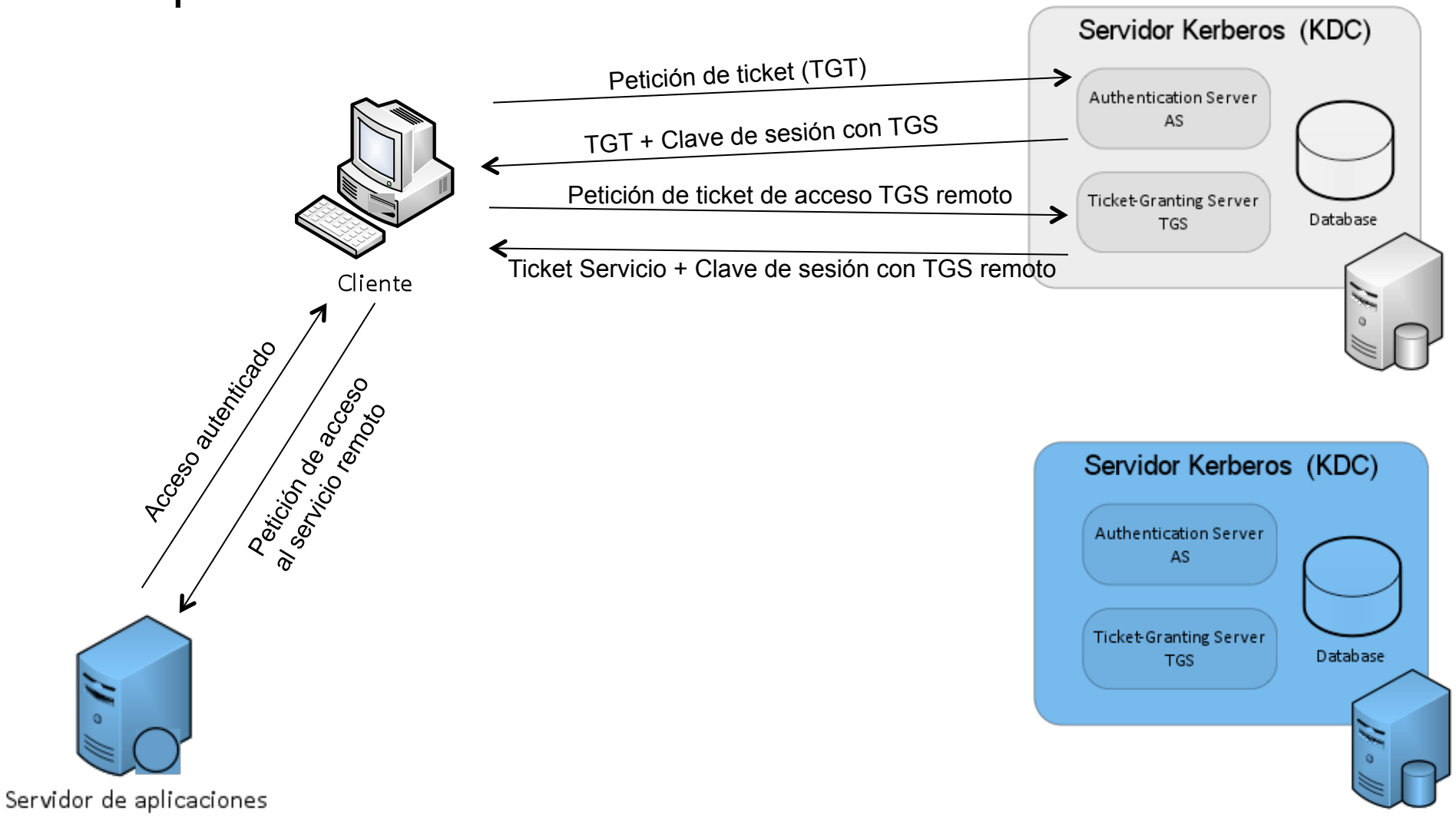
Protocolo versión 4

- Soporte multi-dominio



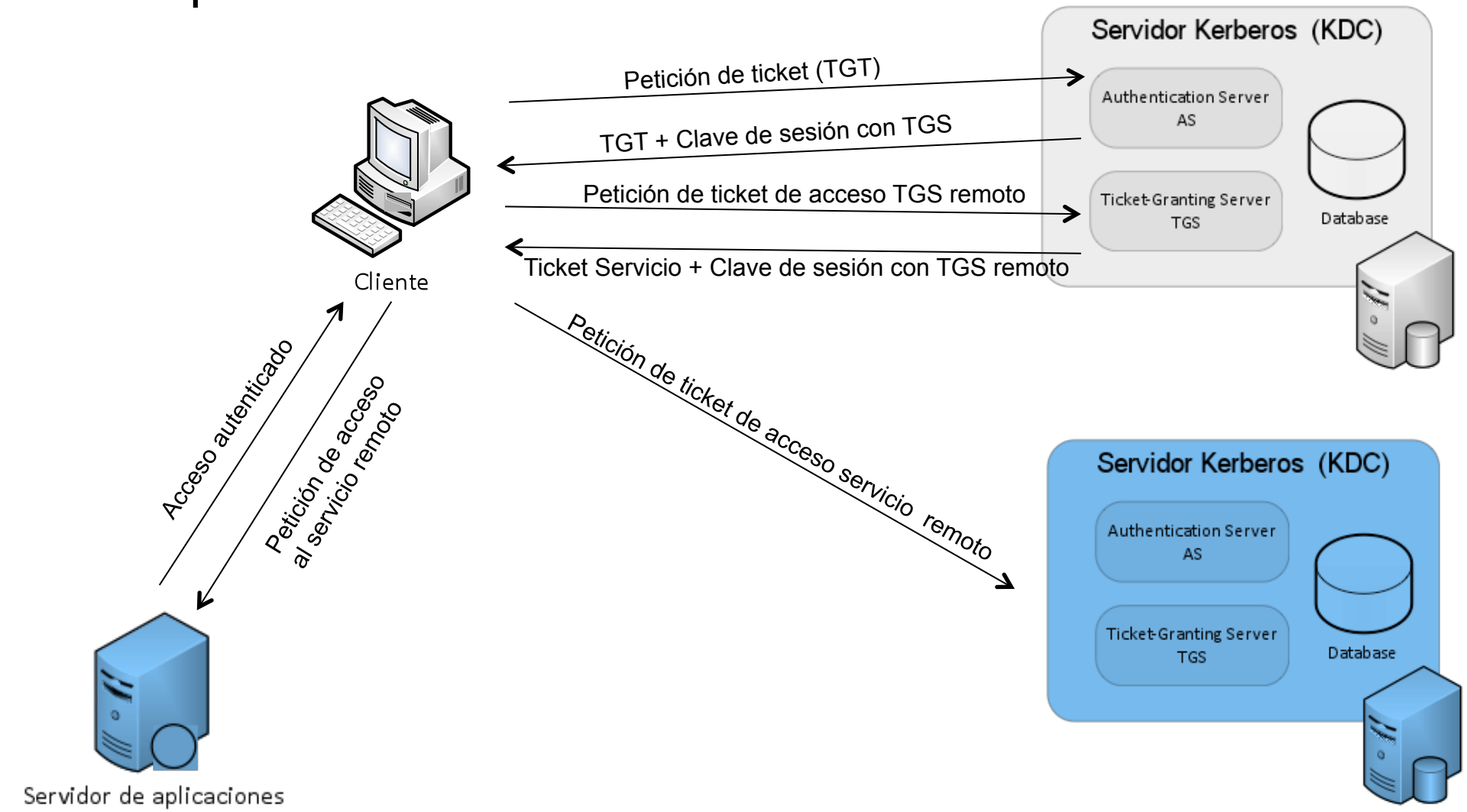
Protocolo versión 4

- Soporte multi-dominio



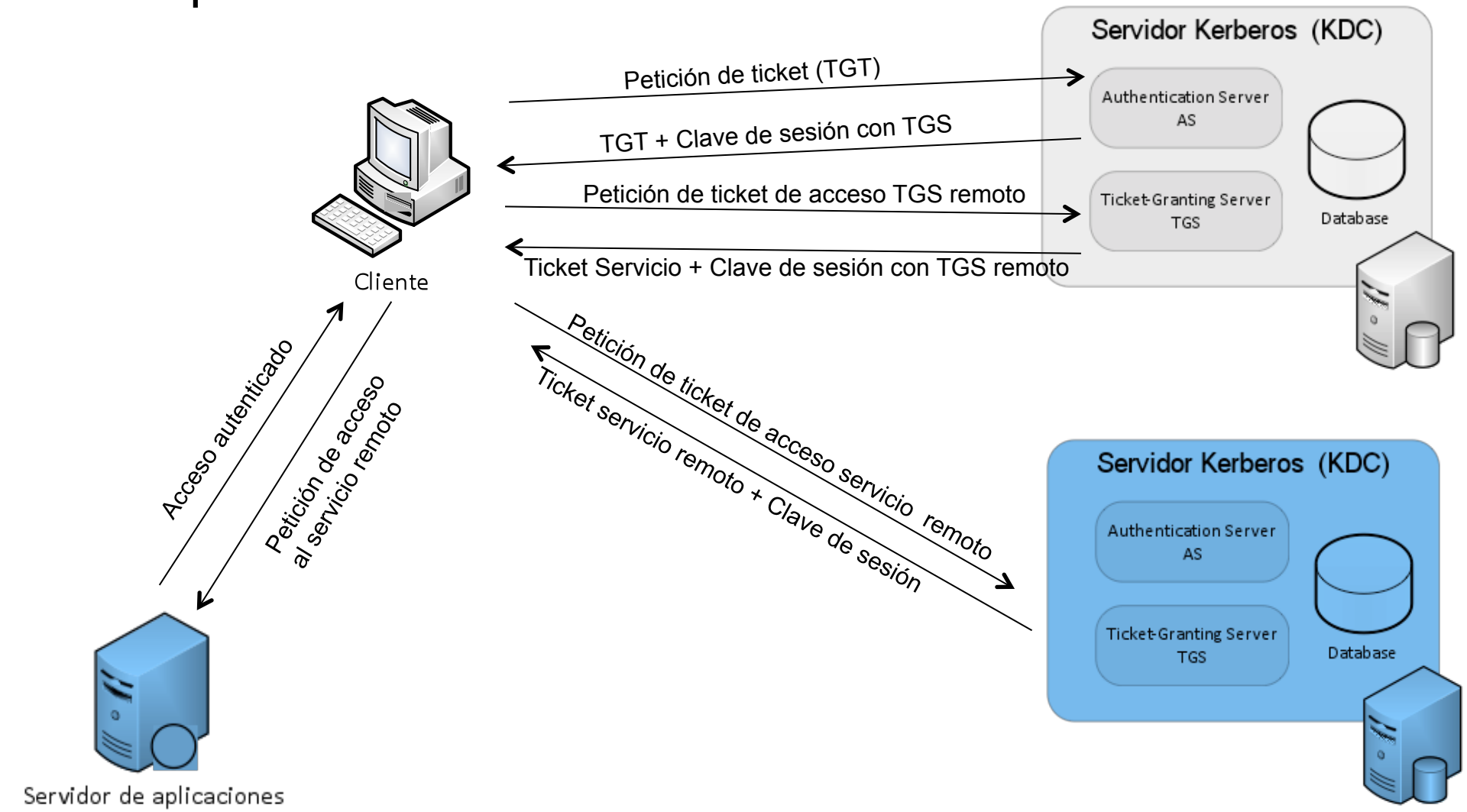
Protocolo versión 4

- Soporte multi-dominio

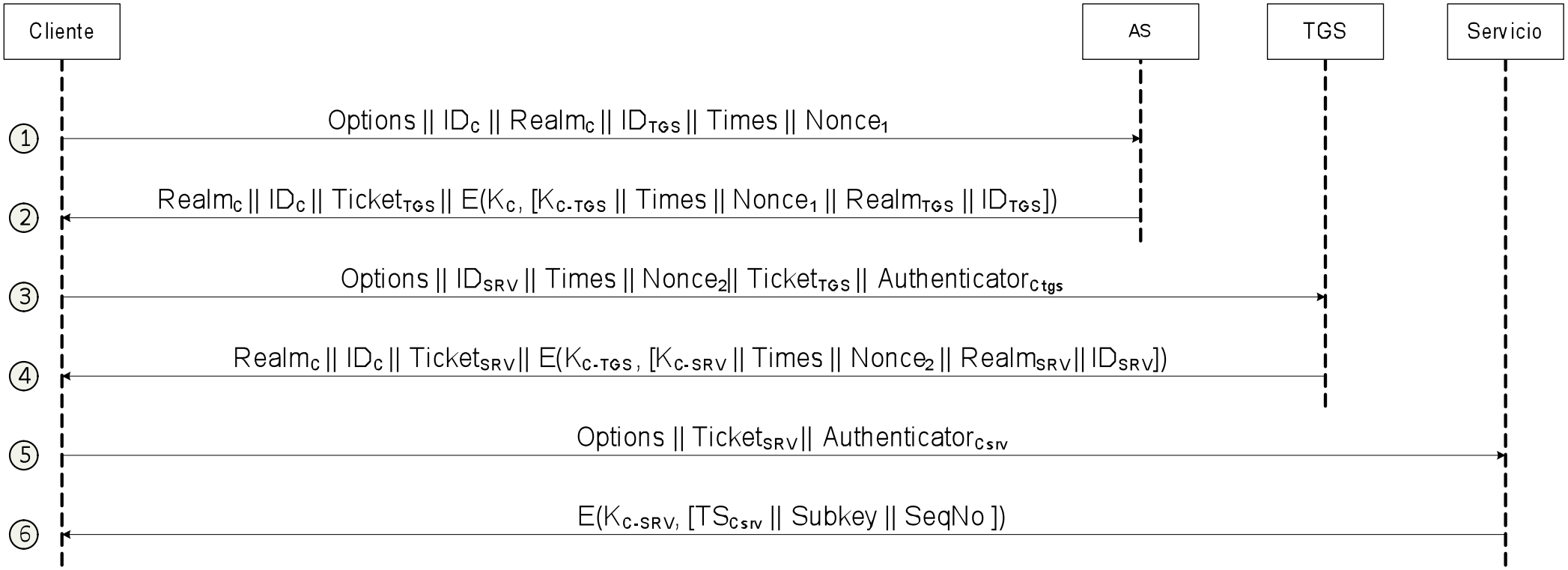


Protocolo versión 4

- Soporte multi-dominio



Protocolo (versión 5)



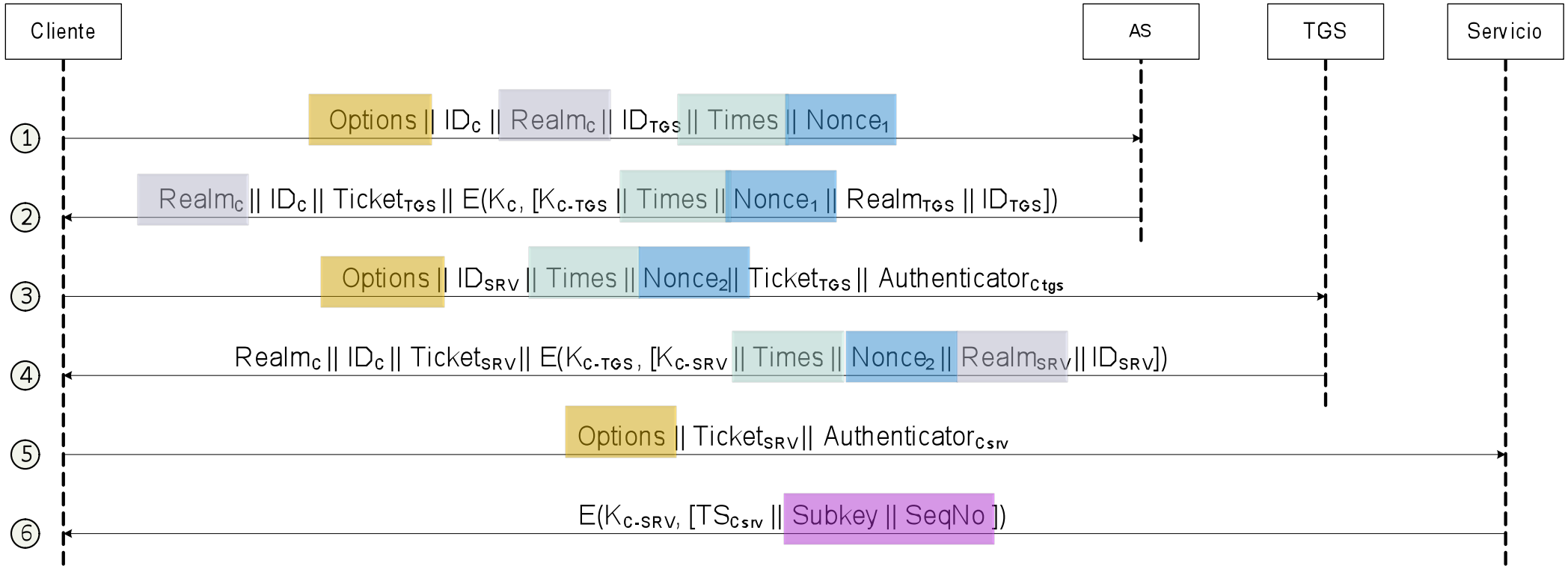
$Ticket_{TGS}=E(K_{TGS}, [Flags || K_{C-TGS} || Realm_C || ID_C || @C || ID_{TGS} || Times])$

$Authenticator_{Ctgs}=E(K_{C-TGS}, [ID_C || Realm_C || TS_{Ctgs}])$

$Ticket_{SRV}=E(K_{SRV}, [Flags || K_{C-TGS} || Realm_C || ID_C || @C || Times])$

$Authenticator_{SRV}=E(K_{C-SRV}, [ID_C || Realm_C || TS_{Csrv} || Subkey || SeqNo])$

Protocolo (versión 5)



$Ticket_{TGS}=E(K_{TGS}, [Flags || K_{C-TGS} || Realm_C || ID_C || @C || ID_{TGS} || Times])$

$Authenticator_{Ctgs}=E(K_{C-TGS}, [ID_C || Realm_C || TS_{Ctgs}])$

$Ticket_{SRV}=E(K_{SRV}, [Flags || K_{C-TGS} || Realm_C || ID_C || @C || Times])$

$Authenticator_{SRV}=E(K_{C-SRV}, [ID_C || Realm_C || TS_{Csrv} || Subkey || SeqNo])$

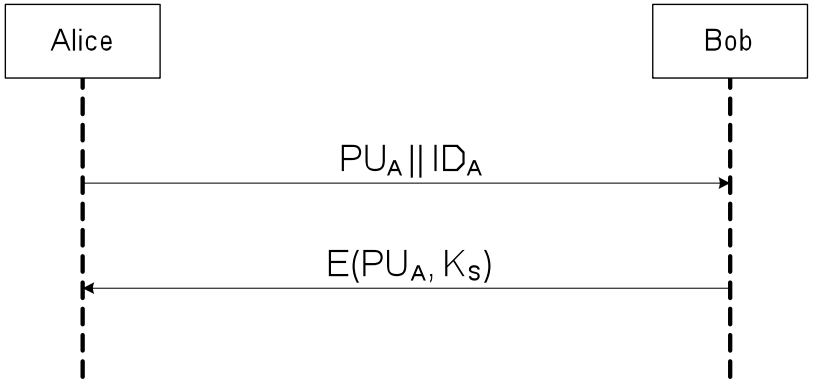
Índice

- Qué es la autenticación
- Modelos de autenticación
  - Intercambios de autenticación
- Gestión de claves
  - Generación
  - Metodologías de distribución
- Kerberos
- Certificación digital - Infraestructura de clave pública
  - Certificado
  - Gestión de certificados
  - Uso de certificados
  - Marco legal

Criptografía de clave pública

- Su ineficiencia computacional hace que se usen principalmente en distribución de claves y autenticación

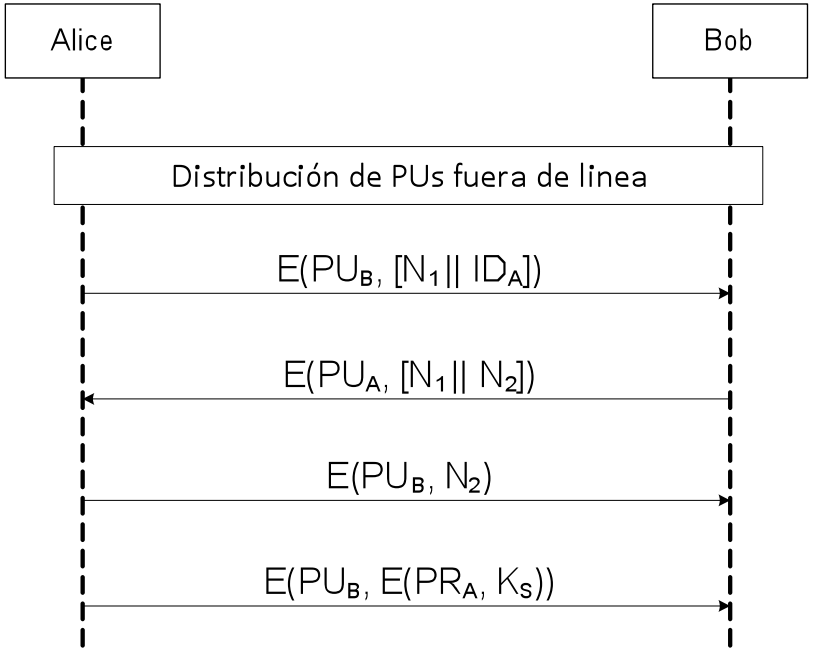
- Autenticación entre extremos



Criptografía de clave pública

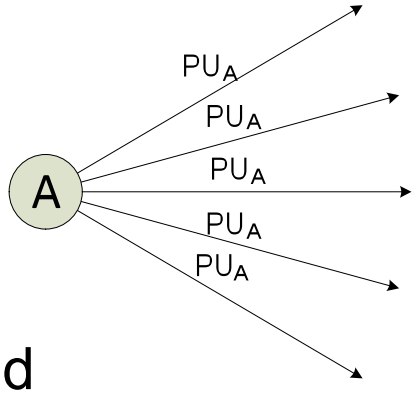
- Su ineficiencia computacional hace que se usen principalmente en distribución de claves y autenticación

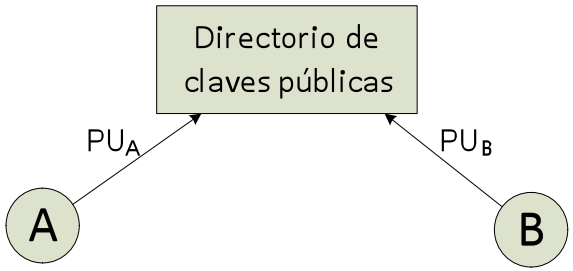
- Autenticación entre extremos

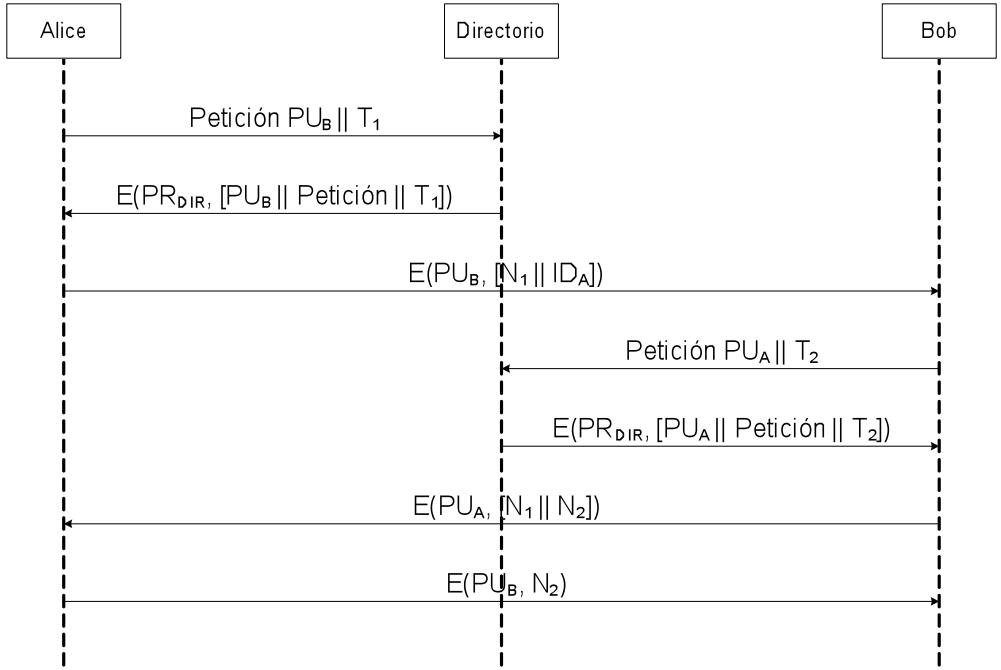


Distribución de claves públicas

- Anuncios
  - Adjunta a mensaje
  - Metodología descontrolada
- Directorio de claves
  - Base de claves vinculadas a identidad

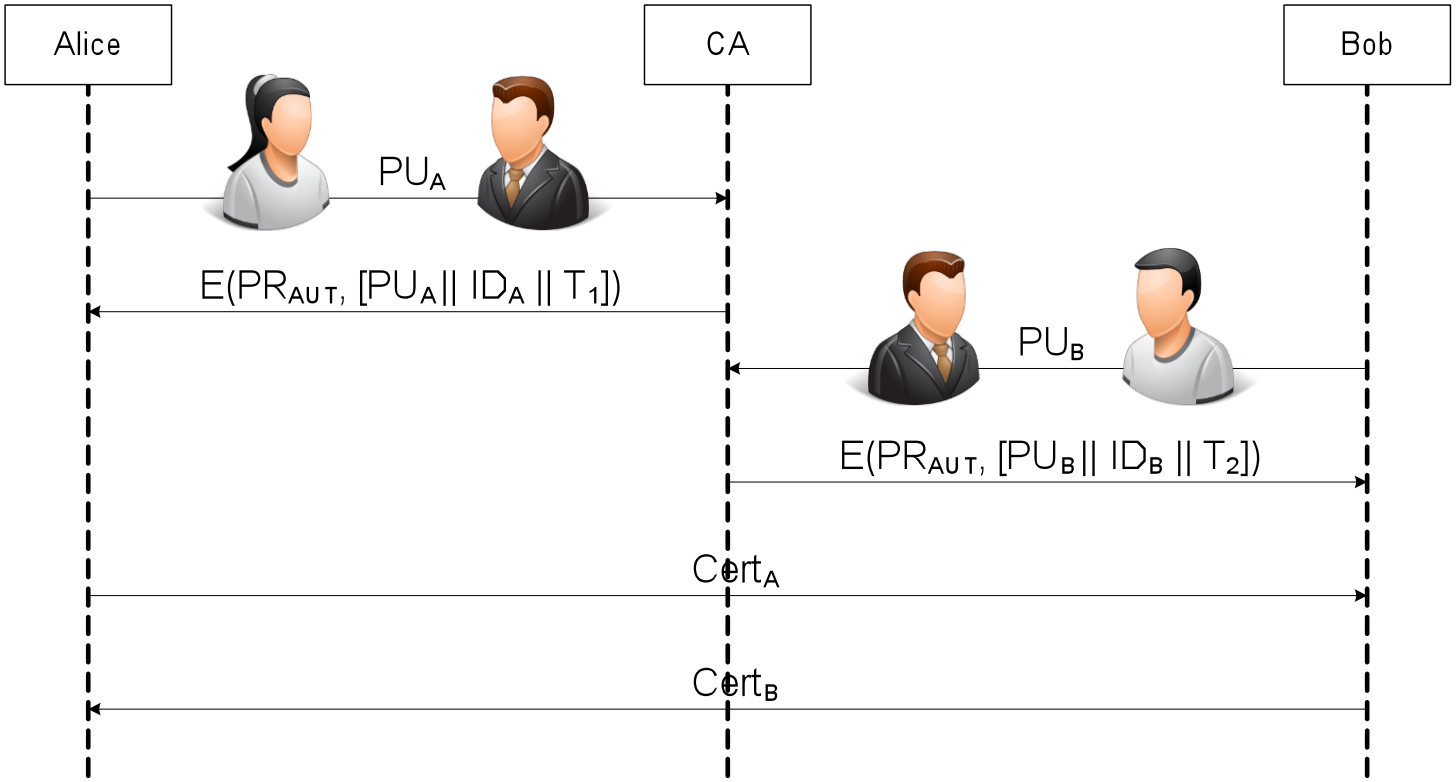






Distribución de claves públicas

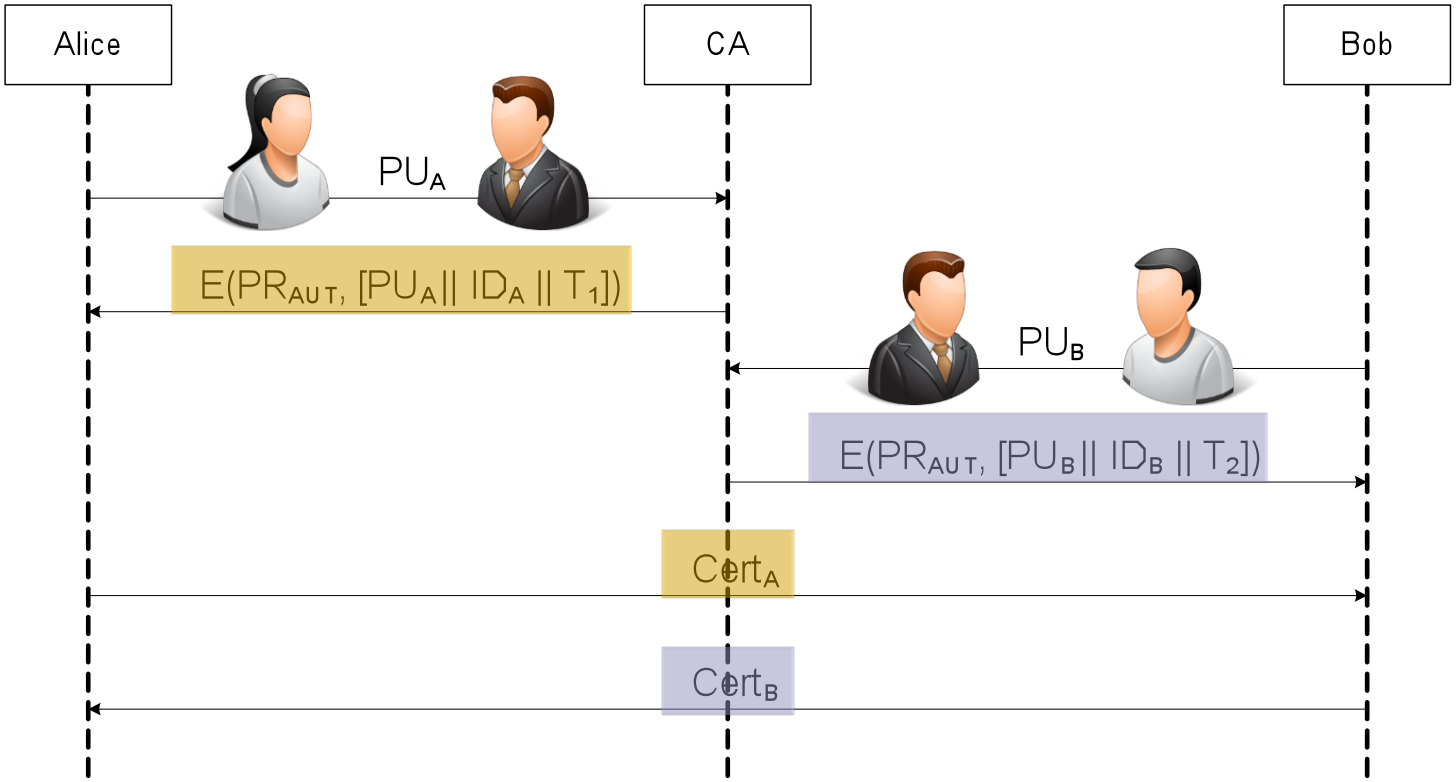
- Autoridad de certificación



$$Cert_X = E(PR_{AUT}, [PU_X || ID_X || T_X])$$

Distribución de claves públicas

- Autoridad de certificación



$$Cert_X = E(PR_{AUT}, [PU_X || ID_X || T_X])$$

Distribución de claves públicas

- Requerimientos de un certificado
  - Cualquiera puede leerlo y extraer la identidad del dueño y su clave pública.
  - Cualquiera debe poder verificar que el certificado ha sido emitido por una entidad de confianza o autoridad de certificación.
  - Solo una autoridad de certificación puede crear, actualizar o revocar certificados.
  - Cualquiera puede verificar la validez del certificado

Distribución de claves públicas

- Requerimientos de un certificado
  - Cualquiera puede leerlo y extraer la identidad del dueño y su clave pública.
  - Cualquiera debe poder verificar que el certificado ha sido emitido por una entidad de confianza o autoridad de certificación.
  - Solo una autoridad de certificación puede crear, actualizar o revocar certificados.
  - Cualquiera puede verificar la validez del certificado

Infraestructura de clave pública

PKI, Public Key Infraestructure

Infraestructura de clave pública

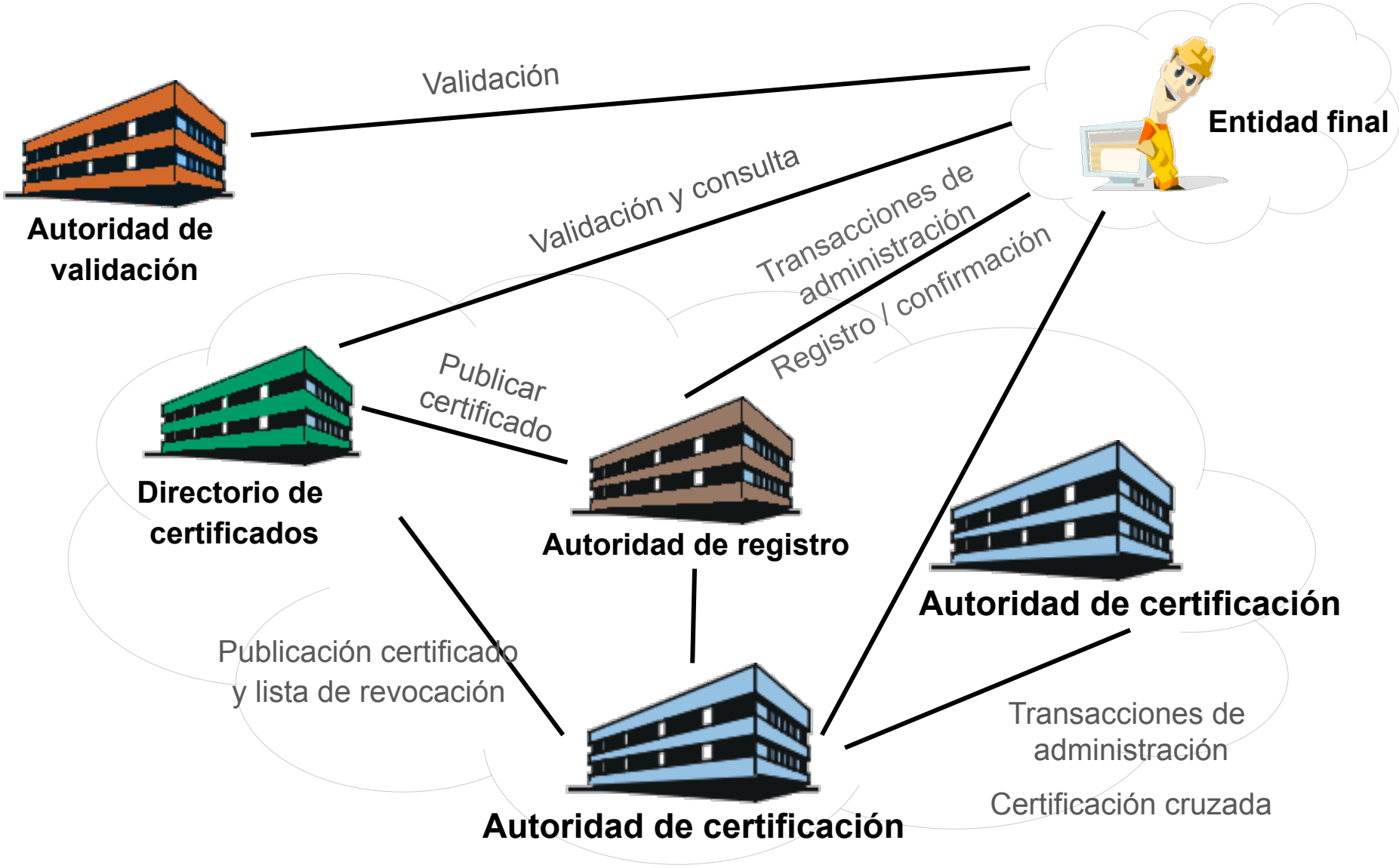
- Conjunto de dispositivos, aplicaciones, personas, políticas y procedimientos que son necesarios para crear, administrar, distribuir y revocar certificados basados en criptografía de clave pública.

Entidades

- Titulares de certificados
  - Entidades finales o sujetos, personas, función ejercida o aplicaciones
- Autoridad de certificación (CA, Certification Authority)
  - Gestión de certificados
- Autoridad de registro (RA, Registration Authority)
  - Autoriza la asociación entre una clave pública y el titular de un certificado
- Directorio de certificados
  - Almacenan y distribuyen certificados y estados (expirado, revocado, etc.)
- Autoridad de validación (Validation Authority)
  - Suministra información en tiempo real acerca del estado de un certificado
- Autoridad de sellado de tiempos (TSA, Timestamping Authority)
  - Da fe de que un determinado dato existe en un momento concreto

Funcionamiento

Infraestructura de clave pública



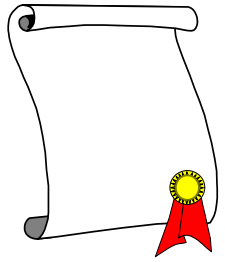
Funcionamiento

- Un usuario se registra para obtener un certificado
- La RA captura la información de registro y genera las claves
- Se realiza la petición de certificado a la CA, quien firma y valida la petición realizada
- Se envía el certificado a la RA quien se lo entrega al usuario
- El certificado está ya emitido
- La CA publica el certificado en un directorio

- Las relaciones de confianza entre los titulares y usuarios de certificados existen por la confianza en la CA como TTP

Certificados

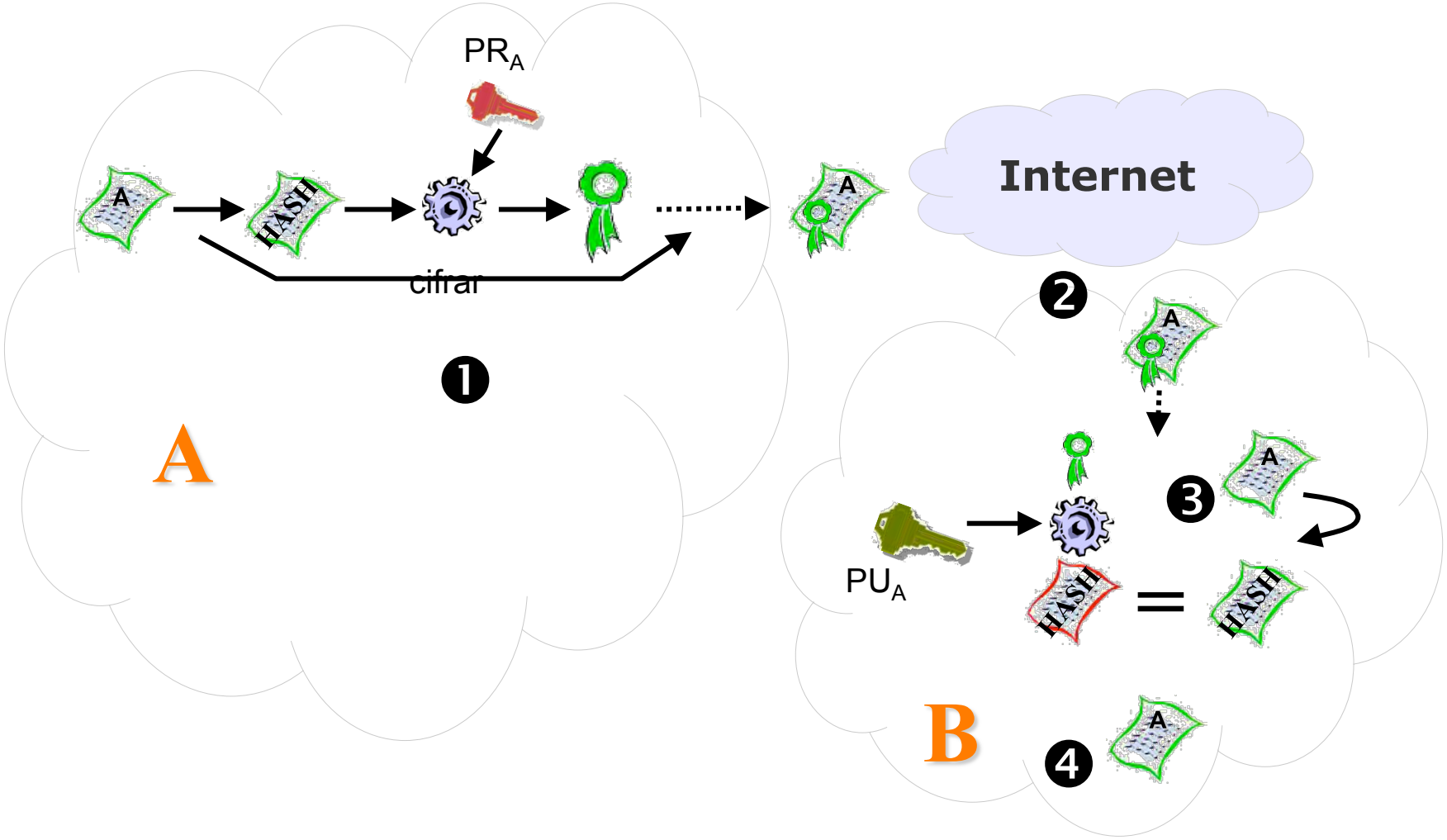
- Prueba de la correspondencia entre el titular y clave pública avalada por una TTP
- Tipos
  - Certificados de servidor
  - Certificados personales
  - Certificados de entidad/organización
  - Certificados de software/desarrollador



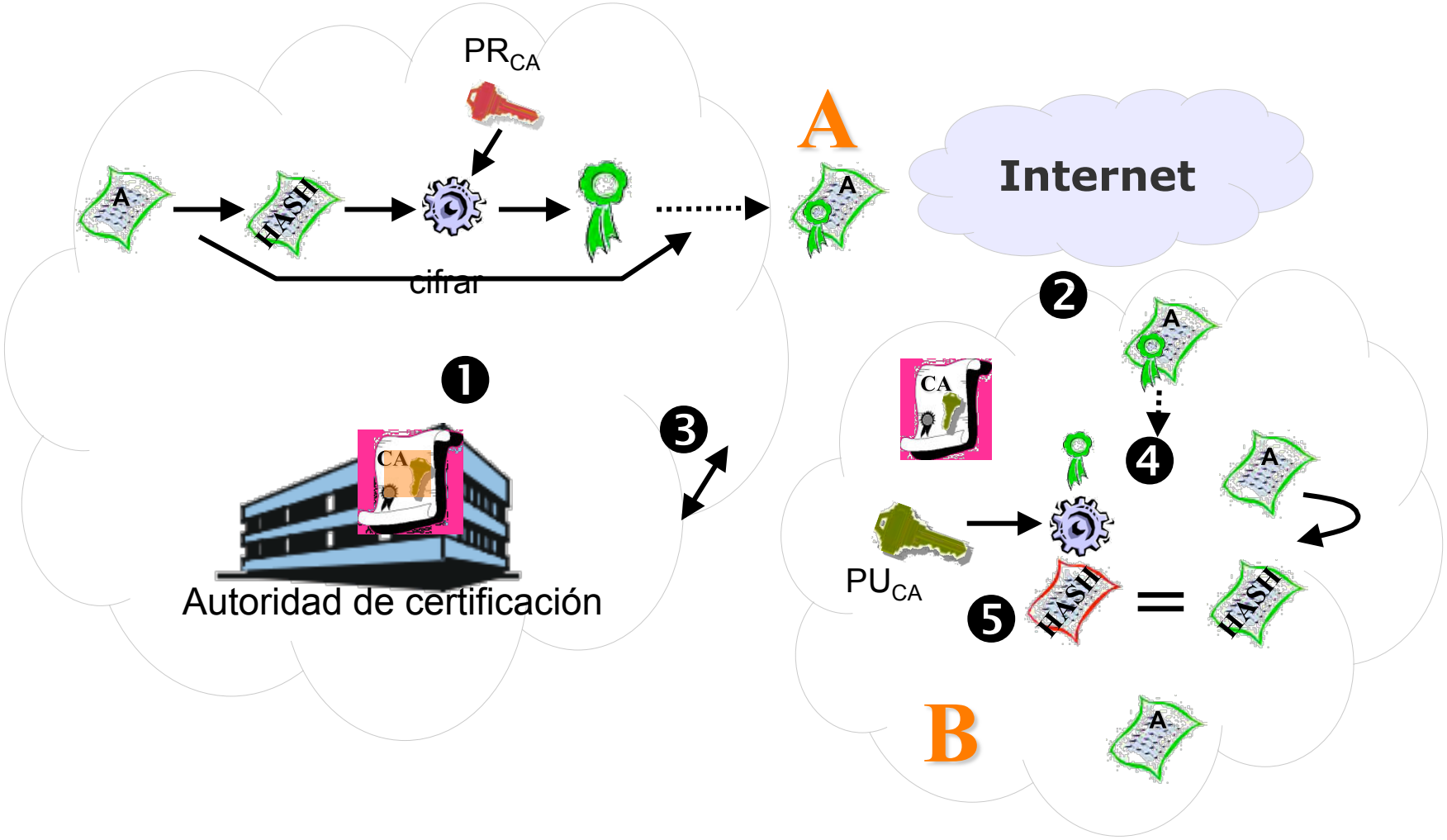
- X.509 es el formato universalmente aceptado (RFC 5280)
  - Considera la existencia de una estructura jerárquica de confianza
  - Usado en S/MIME, IPSec, SSL/TLS, …
  - Recomendaciones sobre algoritmos, pero no fija algoritmos
  - Desde v3 permite extender de manera flexible el contenido del certificado

Firma digital

Infraestructura de clave pública

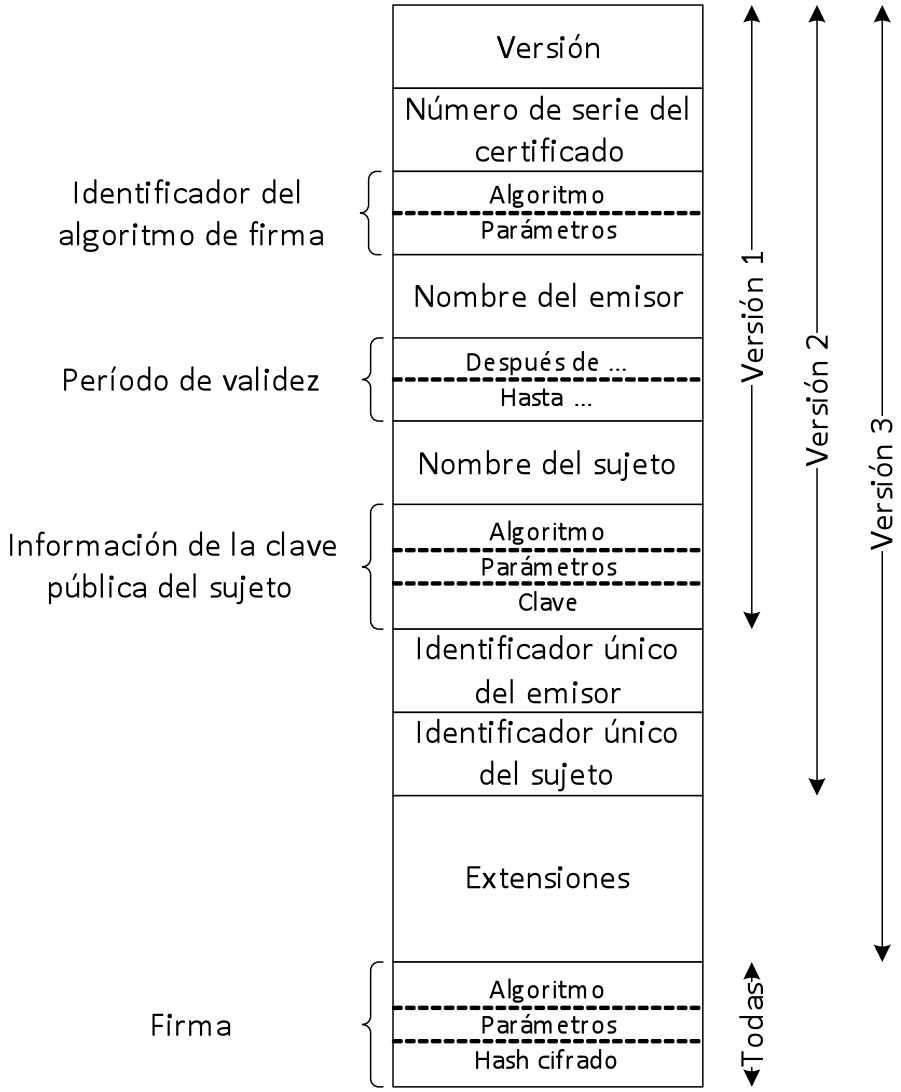


Generación del certificado



Certificados X.509

Infraestructura de clave pública

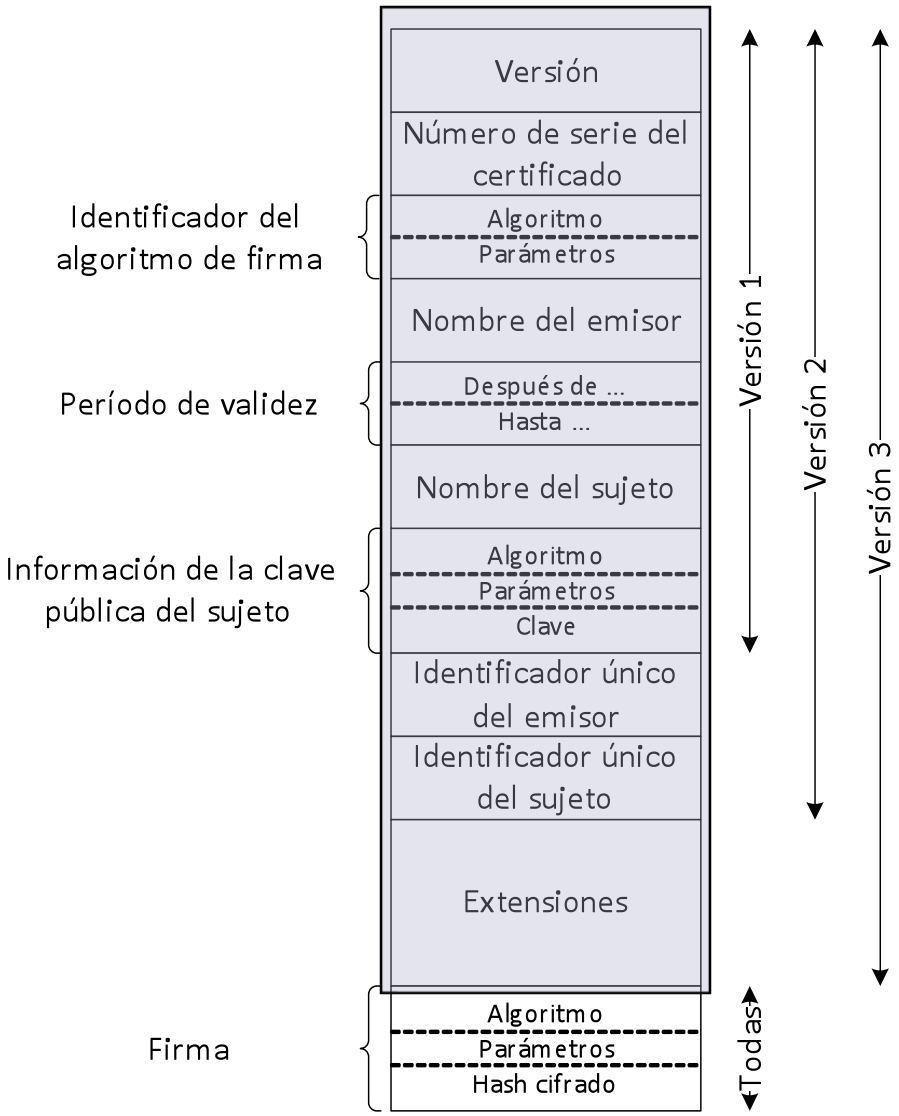



```
Certificate  ::=  SEQUENCE  {
        tbsCertificate       TBSCertificate,
        signatureAlgorithm   AlgorithmIdentifier,
        signatureValue       BIT STRING  }

TBSCertificate  ::=  SEQUENCE  {
        version         [0]  EXPLICIT Version DEFAULT v1,
        serialNumber         CertificateSerialNumber,
        signature            AlgorithmIdentifier,
        issuer               Name,
        validity             Validity,
        subject              Name,
        subjectPublicKeyInfo SubjectPublicKeyInfo,
        issuerUniqueID  [1]  IMPLICIT UniqueIdentifier OPTIONAL,
                             -- If present, version MUST be v2 or v3
        subjectUniqueID [2]  IMPLICIT UniqueIdentifier OPTIONAL,
                             -- If present, version MUST be v2 or v3
        extensions      [3]  EXPLICIT Extensions OPTIONAL
                             -- If present, version MUST be v3
        }
```

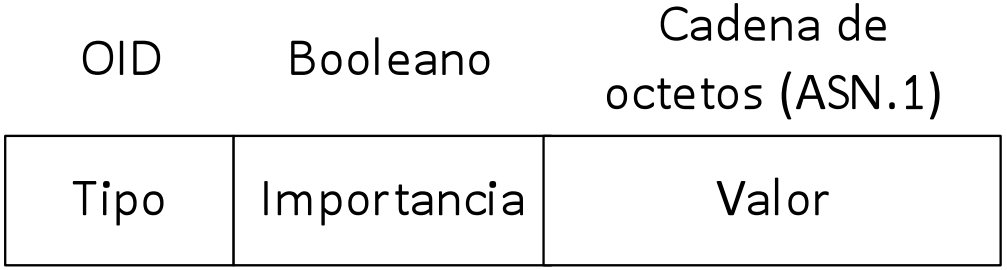
Notación en ASN.1

Certificados X.509



- Algoritmos definidos en
  - RFC3279 RFC4055 y RFC4491
- Cálculo de la firma
  - Hash
    - MD2, MD5
    - SHA-1,
    - SHA-224,SHA-256,SHA-384,SHA-512
    - …
  - Cifrado
    - RSA, DSA, Curvas elípticas
- Algoritmos de clave pública
  - RSA, DSA, KEA, Curvas elípticas

Certificados X.509 - Extensiones



- Estándar
  - Authority Key Identifier
  - Subject Key Identifier
  - Key Usage
  - Certificate Policies
  - Policy Mappings
  - Subject Alternative Name
  - Issuer Alternative Name
  - Subject Directory Attributes
  - Basic Constraints
  - Name Constraints
  - Policy Constraints
  - Extended Key Usage
  - CRL Distribution Points
  - Inhibit anyPolicy
  - Freshest CRL (Delta CRL Distribution Point)
- Privada
  - Authority Information Access
  - Subject Information Access

Almacenamiento de certificados X.509

- .PEM (Privacy Enhanced Mail)
  - Codificación en Base64
  - Entre "-----BEGIN CERTIFICATE-----" y "-----END CERTIFICATE-----“
  - Formato con el que representar claves y otros (BEGIN/END)
- .CER, .DER
  - Extensión de formato BER (Basic Encoding Rules)
  - Puede contener toda la cadena de certificación
- .P7B, .P7B
  - Estructurados según formato PCKS#7
  - Solo permite datos firmados – certificados o CRL
- .P12, PFX
  - Estructurados según formato PKCS#12
  - Diseñado para contener certificado de servidor, certificados intermedios y la clave privada en un fichero cifrado

Certificados X.509 – Usuario

Infraestructura de clave pública

```
Data:
    Version: 3 (0x2)
    Serial Number:
        28:ff:45:13:38:33:3e:91:3a:dc:b8:45:df:1b:ca:98
Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=NL, O=TERENA, CN=TERENA Personal CA
    Validity
        Not Before: Jan 21 00:00:00 2014 GMT
        Not After : Jan 20 23:59:59 2017 GMT
    Subject: C=ES, O=Universidad, CN=XXXXXX /unstructuredName=XXX XXX@domain.com
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
            Public-Key: (2048 bit)
            Modulus:
                00:b6:a8:53:df:a6:b8:c3:8d:fa:93:56:e8:0f:f3:
                ..................................................
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Authority Key Identifier:
            keyid:63:4D:43:5A:19:48:3F:C4:46:C1:02:BA:BF:EE:0E:C5:82:B7:66:A6
        X509v3 Subject Key Identifier:
            8E:4D:03:B7:61:65:C0:0A:B6:37:8D:10:32:DB:4F:DD:37:93:B0:1B
        X509v3 Key Usage: critical
            Digital Signature, Key Encipherment
        X509v3 Basic Constraints: critical
            CA:FALSE
        X509v3 Extended Key Usage:
            E-mail Protection, TLS Web Client Authentication
        X509v3 Certificate Policies:
            Policy: 1.3.6.1.4.1.6449.1.2.2.29
        X509v3 CRL Distribution Points:
            Full Name:
              URI:http://crl.tcs.terena.org/TERENAPersonalCA.crl

Authority Information Access:
    CA Issuers - URI:http://crt.tcs.terena.org/TERENAPersonalCA.crt
    OCSP - URI:http://ocsp.tcs.terena.org
            X509v3 Subject Alternative Name:
    email:XXXX.XXXXX@domain.com
Signature Algorithm: sha1WithRSAEncryption
         05:fa:2d:30:70:a4:8f:fb:12:6c:4b:75:20:ee:3f:3e:22:ca:
         ..................................................
```

Certificados X.509 – CA intermedia

Infraestructura de clave pública

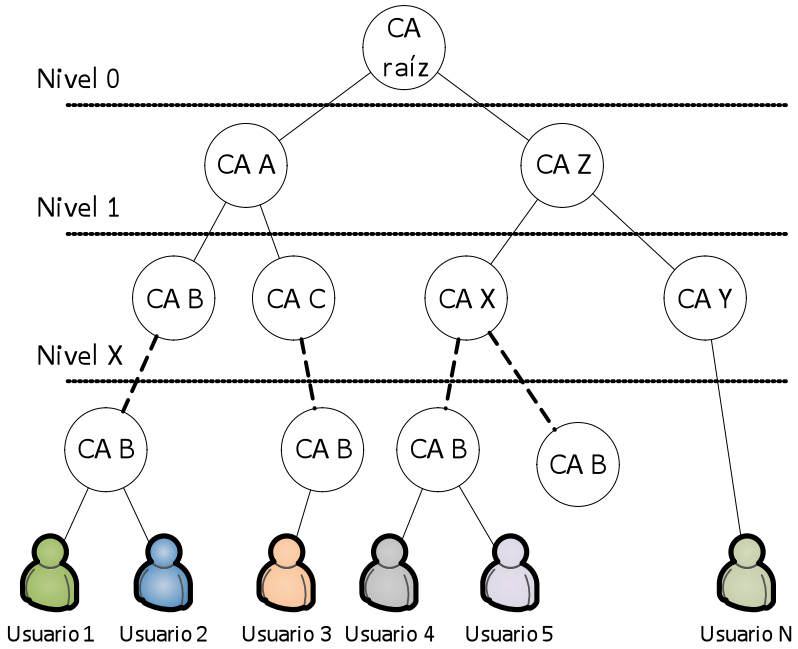
```
Data:
    Version: 3 (0x2)
    Serial Number:
        73:fe:57:fa:df:b8:c5:08:81:7b:66:b9:6b:f0:2d:ef
Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=US, ST=UT, L=Salt Lake City, O=The USERTRUST Network, OU=http://www.usertrust.com,
            CN=UTN-USERFirst-Client Authentication and Email
    Validity
        Not Before: May 18 00:00:00 2009 GMT
        Not After : Dec 31 23:59:59 2028 GMT
    Subject: C=NL, O=TERENA, CN=TERENA Personal CA
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
            Public-Key: (2048 bit)
            Modulus:
                00:c8:15:d9:f5:33:6a:23:a1:90:0d:cf:bb:05:44:
                ..........................................
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Authority Key Identifier:
            keyid:89:82:67:7D:C4:9D:26:70:00:4B:B4:50:48:7C:DE:3D:AE:04:6E:7D
        X509v3 Subject Key Identifier:
            63:4D:43:5A:19:48:3F:C4:46:C1:02:BA:BF:EE:0E:E5:82:B7:66:A6
        X509v3 Key Usage: critical
            Certificate Sign, CRL Sign
        X509v3 Basic Constraints: critical
            CA:TRUE, pathlen:0
        X509v3 Certificate Policies:
            Policy: 1.3.6.1.4.1.6449.1.2.2.29
        X509v3 CRL Distribution Points:
            Full Name:
              URI:http://crl.usertrust.com/UTN-USERFirst-ClientAuthenticationandEmail.crl
        Authority Information Access:
            CA Issuers - URI:http://crt.usertrust.com/UTNAAAClient_CA.crt
            OCSP - URI:http://ocsp.usertrust.com
Signature Algorithm: sha1WithRSAEncryption
     06:2b:a9:53:2f:13:dc:5c:39:16:cc:86:9f:5e:4c:7b:72:fb:
     ..................................................
```

Certificados X.509 – ¿CA raíz?

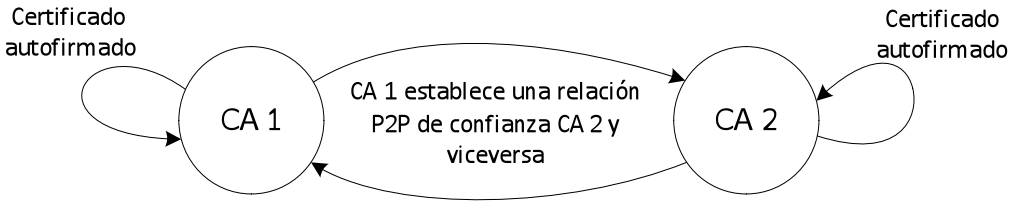

```
Data:
    Version: 3 (0x2)
    Serial Number:
        7c:7c:5d:bd:fd:82:11:1a:73:be:cd:fc:27:01:b8:f0
Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=GB, ST=Greater Manchester, L=Salford, O=Comodo CA Limited, CN=AAA Certificate Services
    Validity
        Not Before: Jan  1 00:00:00 2004 GMT
        Not After : Dec 31 23:59:59 2028 GMT
    Subject: C=US, ST=UT, L=Salt Lake City, O=The USERTRUST Network, OU=http://www.usertrust.com,
             CN=UTN-USERFirst-Client Authentication and Email
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
            Public-Key: (2048 bit)
            Modulus:
                00:b2:39:85:a4:f2:7d:ab:41:3b:62:46:37:ae:cd:
                ........................................
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Authority Key Identifier:
            keyid:A0:11:0A:23:3E:96:F1:07:EC:E2:AF:29:EF:82:A5:7F:D0:30:A4:B4
        X509v3 Subject Key Identifier:
            89:82:67:7D:C4:9D:26:70:00:4B:B4:50:48:7C:DE:3D:AE:04:6E:7D
        X509v3 Key Usage: critical
            Certificate Sign, CRL Sign
        X509v3 Basic Constraints: critical
            CA:TRUE
        X509v3 Certificate Policies:
            Policy: X509v3 Any Policy
        X509v3 CRL Distribution Points:
            Full Name:
              URI:http://crl.usertrust.com/AAACertificateServices.crl
        Authority Information Access:
            OCSP - URI:http://ocsp.usertrust.com
Signature Algorithm: sha1WithRSAEncryption
     a1:33:a1:0c:0a:69:45:62:1f:8e:a7:eb:74:59:a9:9a:8a:6a:
     ................................................
```

Cadena de confianza

- CA con mismas prácticas forman Dominios de Certificación
- Estructura jerárquica



- Certificación cruzada



Validación de certificados

- Necesaria la comprobación del estado de un certificado
  - El certificado ha superado su periodo de validez
  - La clave privada del usuario se ha visto comprometida
  - Cambios en los datos asociados
  - La CA emisora considera que el usuario ha incumplido sus políticas
  - La CA se ha visto comprometida

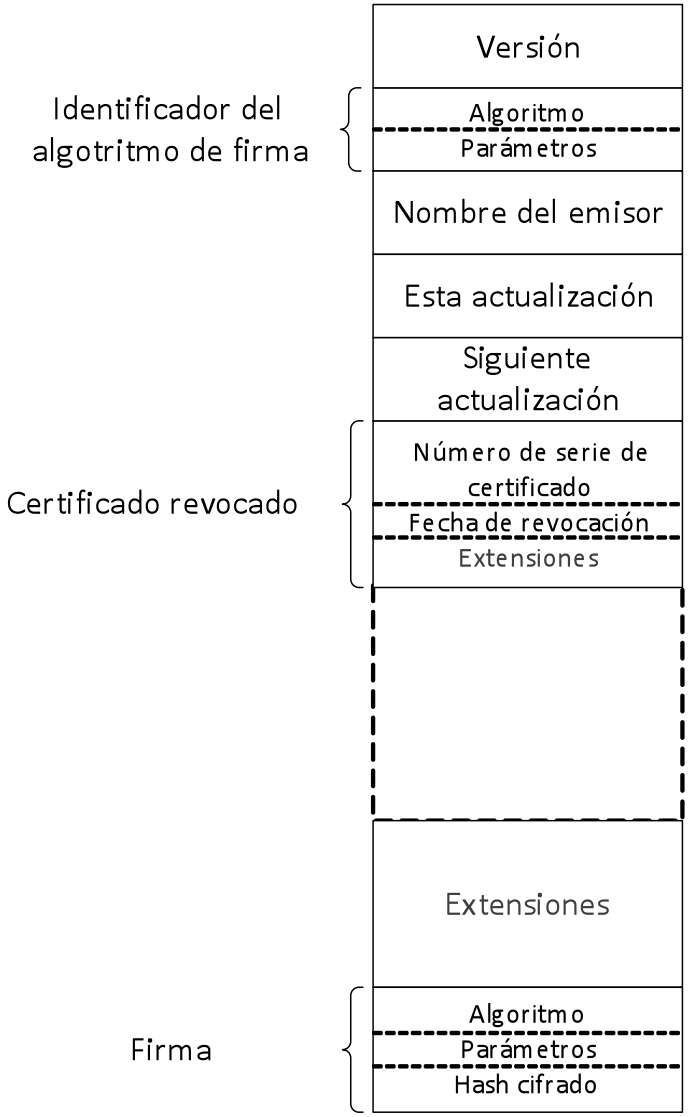
- Opciones
  - Consulta de lista de certificados
  - Consulta de lista de certificados revocados
  - Consulta en tiempo real usando el protocolo OCSP
  - Consulta empleando sistemas propietarios
    - Suelen enmascarar consultas a CRL o la VA a través de OCSP

Listas de revocación (CRL)

- Listado de certificados cuya confianza no se mantiene por parte de la CA
  - Número de serie
  - Fecha de revocación
- Distribución por métodos similares a la distribución de certificados
  - Puntos de distribución incluidos en el campo CRL Distribution Points del certificado X.509 como lugares para consultar las CRL.
  - CRL indirectas que permiten a una CA tener listas de revocación de diferentes CA
  - Delta-CRL que contienen solo los cambios desde la última CRL

Listas de revocación

Infraestructura de clave pública




```
CertificateList  ::=  SEQUENCE  {
    tbsCertList          TBSCertList,
    signatureAlgorithm   AlgorithmIdentifier,
    signatureValue       BIT STRING
}
TBSCertList  ::=  SEQUENCE  {
    version                 Version OPTIONAL,
                                 -- if present, MUST be v2
    signature               AlgorithmIdentifier,
    issuer                  Name,
    thisUpdate              Time,
    nextUpdate              Time OPTIONAL,
    revokedCertificates     SEQUENCE OF SEQUENCE  {
         userCertificate         CertificateSerialNumber,
         revocationDate          Time,
         crlEntryExtensions      Extensions OPTIONAL
                                  -- if present, version MUST be v2
                               }  OPTIONAL,
    crlExtensions           [0]  EXPLICIT Extensions OPTIONAL
                                  -- if present, version MUST be v2
}
```

Notación en ASN.1

Listas de revocación

- Extensiones de una CRL:
  - Authority Key Identifier
  - Issuer Alternative Name
  - CRL Number
  - Delta CRL Indicator
  - Issuing Distribution Point
  - Freshest CRL
  - Authority Information Access

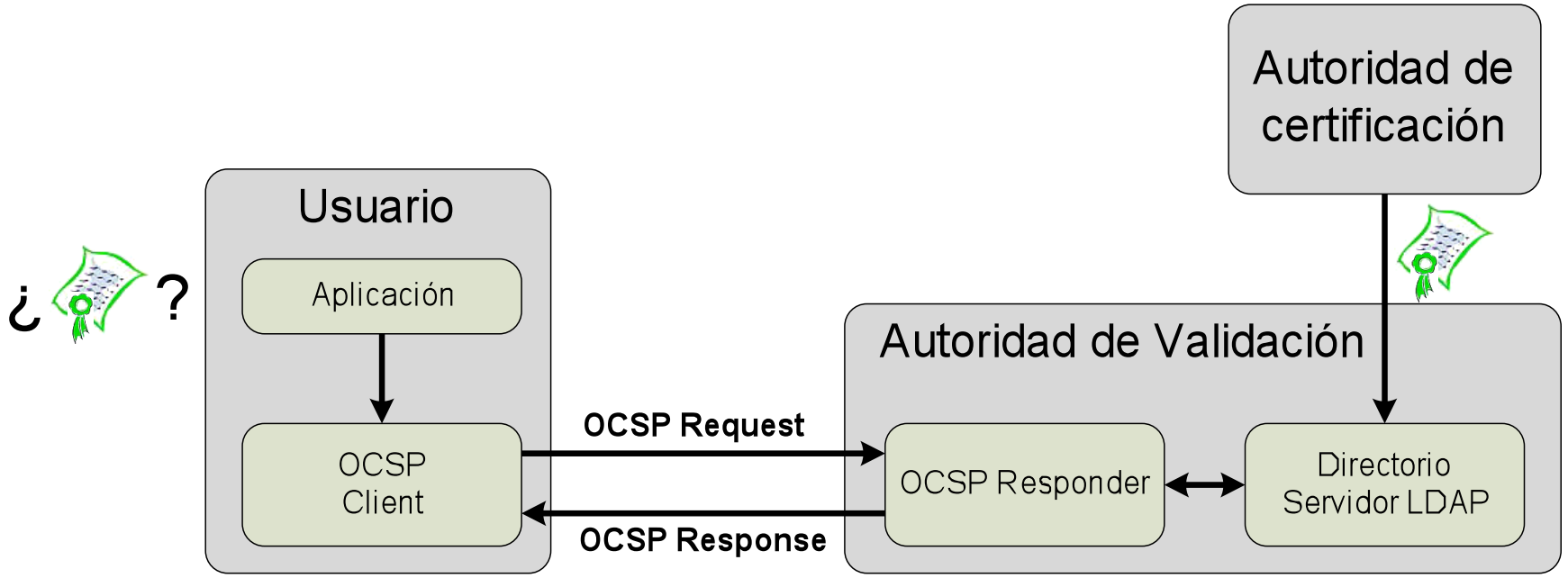
- Extensiones de una entrada de CRL
  - Reason Code
  - Hold Instruction Code
  - Invalidity Date
  - Certificate Issuer

Listas de revocación


```
Certificate Revocation List (CRL):
        Version 1 (0x0)
    Signature Algorithm: sha1WithRSAEncryption
         Issuer: /C=IL/O=StartCom Ltd./OU=Secure Digital Certificate Signing/CN=StartCom Class 1 Primary Intermediate Server
CA
        Last Update: Feb 14 19:01:08 2014 GMT
        Next Update: Feb 16 19:01:08 2014 GMT
Revoked Certificates:
    Serial Number: 0924CD
        Revocation Date: Feb 19 16:01:55 2013 GMT
    Serial Number: 0926DF
        Revocation Date: Feb 15 10:50:13 2013 GMT
 Signature Algorithm: sha1WithRSAEncryption
         9c:22:67:e5:aa:f4:0f:14:a8:dc:4b:5f:64:1f:e6:d2:17:5e:
         ..................................................
         1e:02:34:f4:ab:5d:73:3e:42:93:0a:cd:0a:6b:d6:81:6f:ad:
         07:55:ff:37
-----BEGIN X509 CRL-----
MIJgdjCCX14wDQYJKoZIhvcNAQEFBQAwgYwxCzAJBgNVBAYTAklMMRYwFAYDVQQK
Ew1TdGFydENvbSBMdGQuMSswKQYDVQQLEyJTZWN1cmUgRGlnaXRhbCBDZXJ0aWZp
..........................................................
Juv6NIP830JTIJD2gE5FqWuZ9ALXo6/Dxs8r0LkiR5STvpyH5jeuOvblBilcMJi8
GxWhPB4CNPSrXXM+QpMKzQpr1oFvrQdV/zc=
-----END X509 CRL-----
```

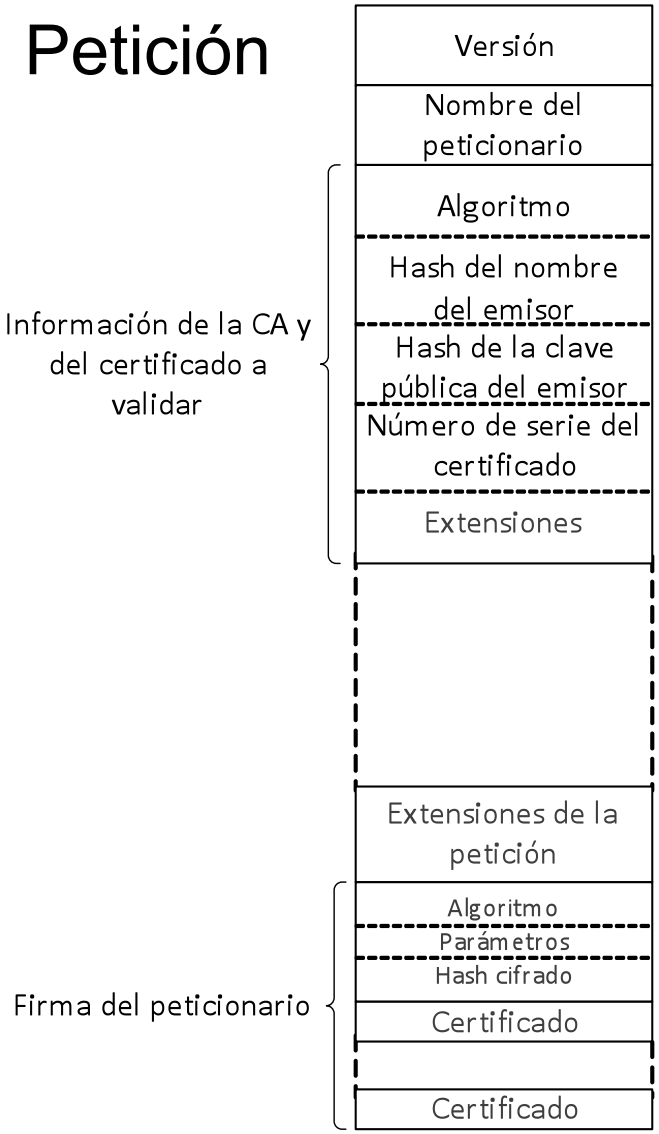
Online Certificate Status Protocol (OCSP)

- Protocolo que permite acceder al estado de un certificado en tiempo real sin necesidad de emplear CRL
- Definido en RFC 6960

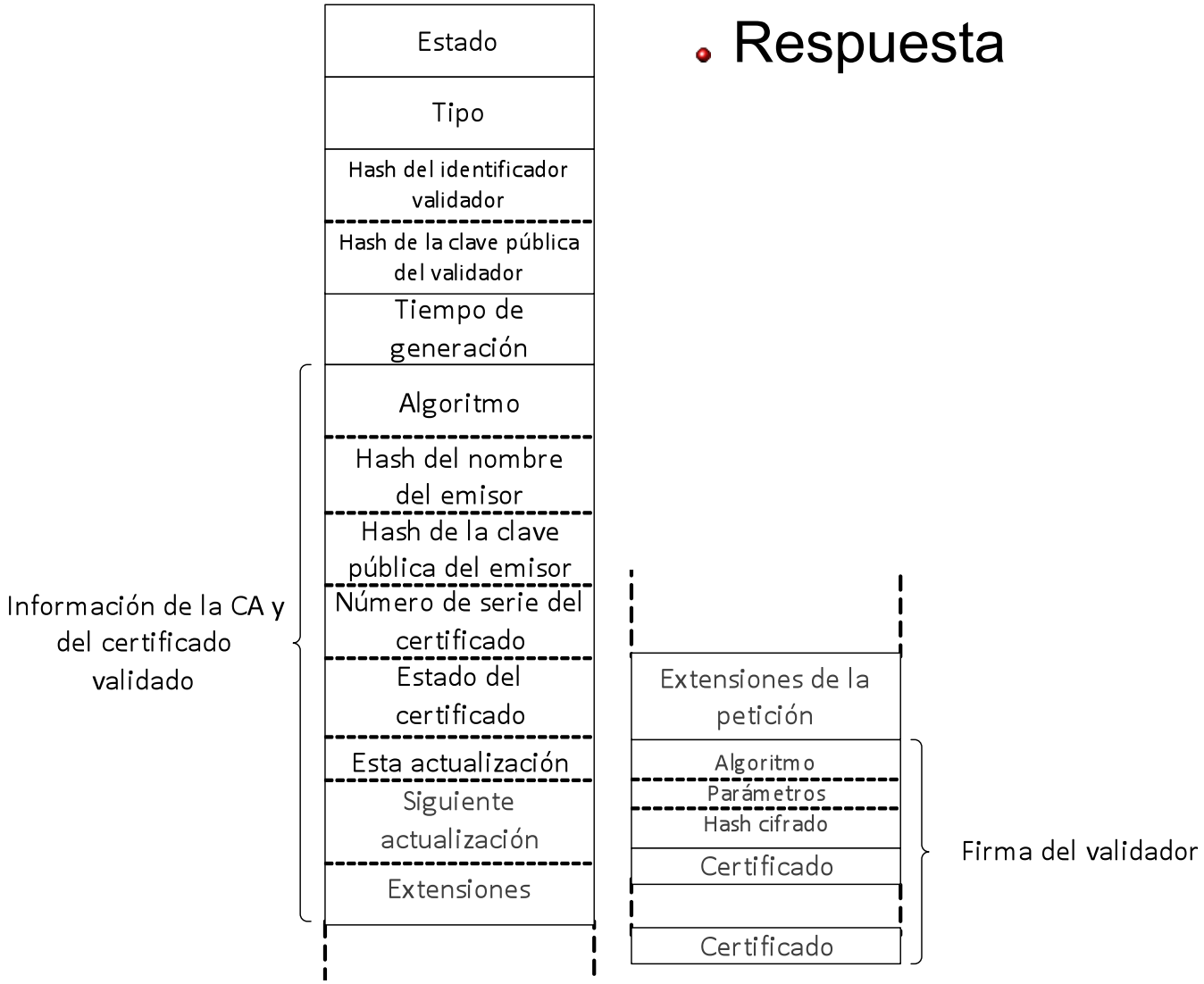


Online Certificate Status Protocol (OCSP)

- Petición



- Respuesta

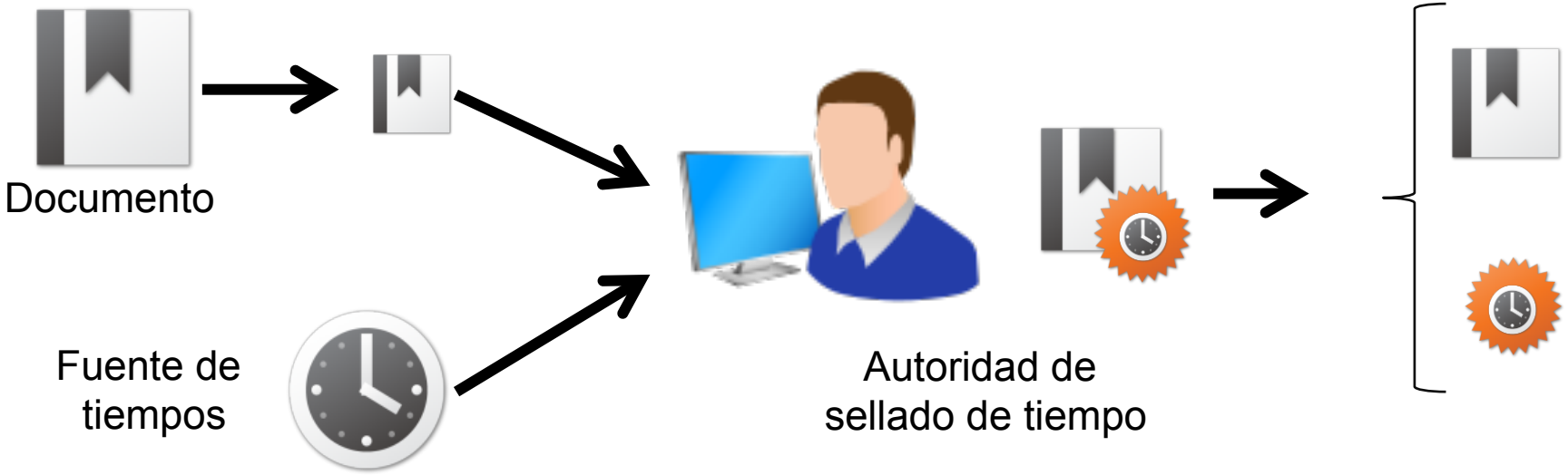


CRL vs OCSP

- OCSP proporciona una mayor eficiencia para redes y clientes con pocos recursos
  - La respuesta OCSP contiene menos información que la normalmente incluida en una CRL
  - Delta-CRL resuelven en parte el problema del volumen de datos de CRL
- CRL tienen que ser analizadas ⇒ recursos computacionales
  - Permiten una mayor velocidad de validación al ser locales.
- OCSP debe ser cacheado para ofrecer la información de CRL
  - CRL contine la información de todos los revocados
- OCSP no tiene por qué transmitir información cifrada o firmada.
  - Revela que alguien está usando un certificado y quiere validarlo

Sellado de tiempo

- La Autoridad de Sellado de Tiempo (TSA) garantiza de forma objetiva y precisa, a través de la entrega de Sellos de Tiempo, la existencia de un dato/información en un instante de tiempo determinado
- Objetivos principales del uso de una TSA
  - Disponer de certeza temporal
  - Custodia de firmas electrónicas



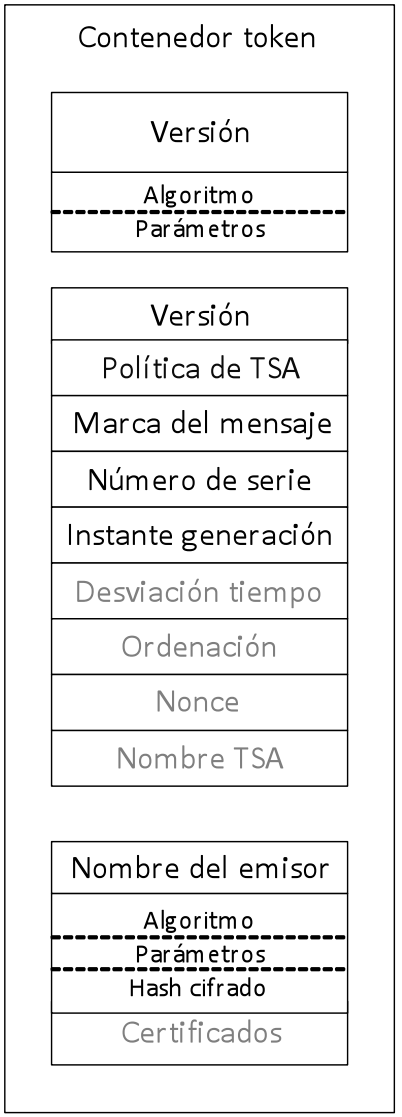
Sellado de tiempo

- Petición

Versión
Marca del mensaje
Política de TSA
Nonce
Petición certificado
Extensiones

- Respuesta

Estado
Descripción estado
Información adicional



Políticas de certificación

- ¿Qué tipos de certificados emitir?
  - Certificados de identidad, de firma, de autorización, de código, …
- Árbol de confianza
  - Varias o una única CA, certificación cruzada con otras, …
- Autoridades de registro
- Procedimientos operativos
  - Cómo se solicitan los certificados
  - Gestión de claves y certificados (generación, distribución, almacenamiento)
    - Si se pueden exportar o archivar las claves privadas, longitud de las claves, ...
  - Tratamiento de la validez
- Provisiones legales
  - Leyes que rijan sanciones, responsabilidades y compromisos

Declaración de prácticas de certificación

- Traslada las políticas de certificación a procedimientos operacionales
  - Indica cuales son las prácticas utilizadas para emitir los certificados.
  - Incluye las características de los equipos, políticas y procedimientos a implantar.

- Política vs CPS (*Certificate Practice Statement*)
  - Una PKI emplea una CP para definir lo que los usuarios deben hacer
    - Una CA usa su CPS para definir como cumple lo que se imponga en una CP
  - CPS es el manual de uso de los poseedores de un certificado
  - La política es importante para la interoperabilidad
  - Una CA puede tener una CPS y varias políticas
    - Certificados para diferentes propósitos
    - Certificados para comunidades diferentes

- Recomendación CPS y CP ⇒ RFC 3647

Hardware vs software criptográfico

- Argumentos sobre el Hardware
  - Velocidad de Proceso: DES y RSA son ineficientes en SW
  - Seguridad Física
    - No poder modificar los algoritmos
    - Almacenamiento seguro de las claves.
  - Certificación: Facilidad de certificación por 3ª parte
  - Instalación: Facilidad de implantación
  - Costes: Alto coste inicial, rápido retorno de la inversión

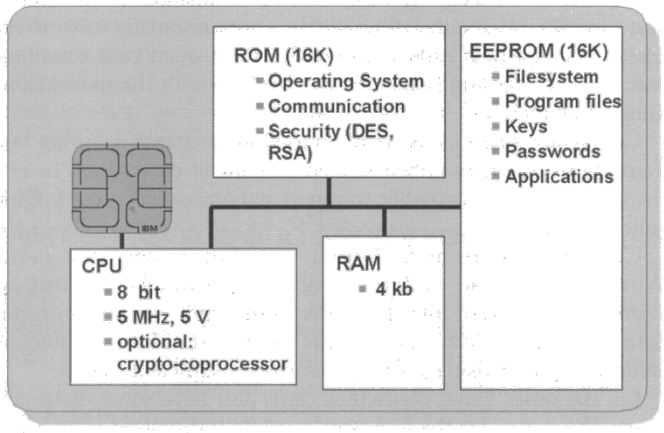
- Argumentos sobre el Software
  - En Contra: Lentitud de proceso, facilidad de manipulación, costes de modificaciones
  - A favor: Flexibilidad, portabilidad, facilidad de uso y de actualización

Hardware criptográfico

- HSM (Hardware Security Module)
- Dispositivos especializados en realizar tareas criptográficas
- Proporcionan
  - Almacenamiento seguro de claves
  - Funciones criptográficas básicas
    - Generación de claves
    - Firma
    - Cifrado
- Tipos
  - Aceleradores de procesamiento
  - Generadores y almacenes de claves
  - Equipos de comunicaciones y VPN
  - Equipos portátiles (tarjetas inteligentes, usb, …)

Tarjeta inteligente

- Plástico con un chip de silicio integrado en ella
  - Diferentes formatos según su uso
- Doble seguridad: tengo y sé
- Capacidades
  - Capacidades de proceso
  - Co-procesador criptográfico
  - Memoria de almacenamiento
  - Interfaces de comunicaciones
    - Con contactos
    - Sin contactos
- Sistemas operativos
  - Monoaplicación o dedicados
  - Multiaplicación: Javacard, Multos, .NET, …



Marco legal de la firma electrónica

Firma electrónica

- Directiva 1999/93/CE
- Ley 59/2003

Protección y procesamiento de datos personales

- Directivas 1995/46/CE, 97/66/EC, 2002/58/CE
- Reglamento (EC) 45/2001
- L.O.P.D. 15/1999 y Real Decreto 994/1999. Ley 32/2003 y 34/2002

Documento Nacional de Identidad

- LO 1/1992, de Protección de la Seguridad Ciudadana
- R.D. 1553/2005. Expedición del DNI y sus certificados electrónicos

- Directiva 2000/31/CE, de 8 de junio de 2000, Directiva sobre el comercio electrónico
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información (LISI)
- Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP)

Ley 59/2003: Articulado

- Artículo 1. Objeto
  - 1. Esta ley regula la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación.
- Artículo 2. Prestadores de servicios de certificación sujetos a esta ley
- Artículo 3. Firma electrónica y documentos firmados electrónicamente
- Artículo 4. Empleo de la firma electrónica en el ámbito de las AAPP
  - 1. Esta ley se aplicará al uso de la firma electrónica en el seno de las Administraciones públicas, sus organismos públicos y las entidades dependientes o vinculadas a las mismas y en las relaciones que mantengan aquéllas y éstos entre sí o con los particulares.(...)
  - 4. La utilización de la firma electrónica en las comunicaciones que afecten a la información clasificada, a la seguridad pública o a la defensa nacional se regirá por su normativa específica.

Ley 59/2003: Definiciones

- Firma electrónica
  - Es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.
- Firma electrónica avanzada
  - Firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.
- Firma electrónica reconocida
  - Firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

Ley 59/2003: Definiciones

- Prestador de servicios de certificación (PSC)
  - Persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.
- Certificado electrónico
  - Un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.
- Certificados reconocidos
  - Certificados electrónicos expedidos por un PSC que cumpla los requisitos establecidos la Ley 59/2003 en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación.