SEGURIDAD DE LA INFORMACIÓN

TEMA 3

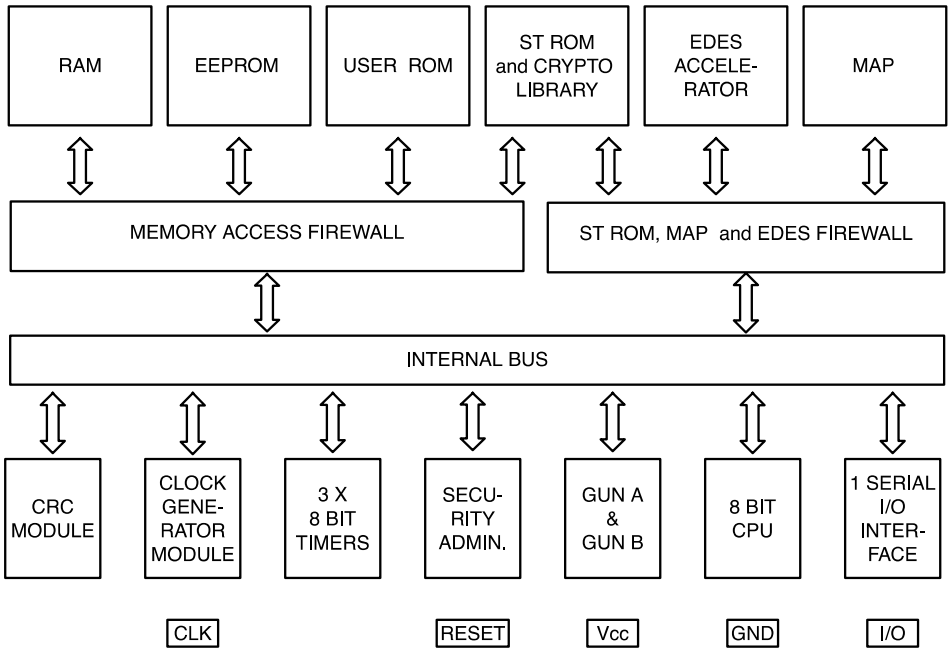
ESQUEMAS, PROTOCOLOS Y MECANISMOS DE SOPORTE

(A LA SEGURIDAD DE APLICACIONES Y DE REDES)

DNI Electrónico (DNI-e)

- El DNI electrónico, a través de las capacidades criptográficas que aporta, permite:
  - **identificación en medios telemáticos**
  - **firmar electrónicamente**
- El DNI-e está dotado con el chip ST19WL34 (STMicroelectronics), compuesto por:
  - microprocesador securizado de 8 bits
  - 6 Kb de memoria RAM
  - 224 KB de memoria ROM para el almacenamiento del sistema operativo y código de programas
  - 34 KB de memoria EEPROM para el almacenamiento de datos personales con tecnología de almacenamiento fiable y código de corrección de errores
- El chip ofrece una retención de datos de al menos 10 años, y una resistencia de 500.000 ciclos de borrado y escritura

- Este chip se caracteriza por incorporar también:
  - procesador aritmético modular (MAP) de 1088 bits para **criptografía de clave publica**
  - motor de aceleración por hardware de los **algoritmos DES y triple-DES**
  - módulo para el cálculo de **funciones CRC**
  - interfaz de entrada/salida serie
  - generador de números aleatorios
  - bus de interconexión interno
  - 3 timers de 8 bits
  - reloj interno



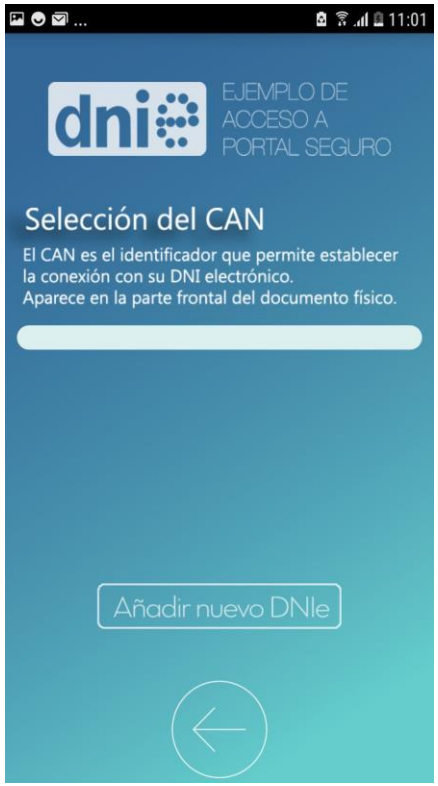
- La tabla muestra algunas medidas de tiempo de la ejecución de operaciones criptográficas

Function	Speed(1)
RSA 1024 bits signature with CRT(2)	85 ms
RSA 1024 bits signature without CRT(2)	282 ms
RSA 1024 bits verification (e='$10001')	5.5 ms
RSA 1024 bits key generation	2.5 s
RSA 2048 bits signature with CRT(2)	570 ms
RSA 2048 bits verification (e='$10001')	91 ms
Triple DES (with enhanced security)	58.0 μs
Single DES (with enhanced security)	43.0 μs

1. Typical values, independent from external clock frequency and supply voltage.
2. CRT: Chinese Remainder Theorem.

- El sistema operativo que gestiona el chip se denomina DNIe v3.0, desarrollado por la FNMT a partir de las especificaciones funcionales de la Dirección General de Policía
  - este sistema operativo ha sido sometido con posterioridad a los perfiles de protección de la certificación *Common Criteria*

Leer DNI-e 3.0 en Android – con NFC



CAN (Card Access Number) es un número que aparece en la parte inferior del DNI 3.0, y corresponde con el número de la tarjeta como medida de seguridad

Componentes del DNI-e

- El DNI-e contiene dos certificados digitales asociados al titular:
  - **certificado de autenticación**: asegura que la comunicación electrónica se realiza con el titular del DNI, pero no demuestra voluntad de firma
    - restringido a operaciones para confirmar la identidad y acceso seguro a sistemas remotos
  - **certificado de firma**: para la firma de documentos, garantizando la integridad del documento y el no repudio de origen

- Cuenta también con un **certificado de componente**, emitido para autenticar al propio chip y cifrar la comunicación con él
  - de forma similar a como se utiliza un certificado SSL en un servidor Web

- El generador interno de números aleatorios origina el par de claves de cada certificado, en presencia del ciudadano:
  - se garantiza que sólo existirá una copia de cada clave privada, y que ésta residirá siempre en el interior del chip

- La información de la **memoria EEPROM** del chip está distribuida en tres zonas, con diferentes niveles y condiciones de acceso
- Las tres son sólo accesibles para realizar **operaciones de lectura**, no siendo posible para el ciudadano escribir o grabar datos
  - **zona pública**: accesible sin restricciones
    - certificado CA emisora
    - claves Diffie-Hellman
    - certificado X.509 de componente
  - **zona privada**: accesible por el ciudadano mediante la utilización de su PIN
    - certificado de autenticación (identificación)
    - certificado de firma
  - **zona de seguridad**: accesible por el ciudadano de forma exclusiva en los puntos de actualización del DNI-e (en las comisarías)
    - datos de filiación del ciudadano
    - fotografía del titular
    - imagen de la firma manuscrita

Smart Card -- el caso del DNI-e

CUERPO NACIONAL DE POLICÍA

GOBIERNO DE ESPAÑA · MINISTERIO DEL INTERIOR · DIRECCIÓN GENERAL DE LA POLICÍA

DNI y Pasaporte

Cuerpo Nacional

Policía Nacional

Ciudadanos · Empr

Inicio / Certificados Electrónicos / Qué son los Certificados Electrónicos

- DNI electrónico
- Obtención del DNI
- Cómo utilizar el DNI
- Guía de referencia básica
- Certificados Electrónicos
  - Qué son los certificados electrónicos
  - Renovación de Certificados
  - Aceptación de los Certificados
  - Autoridades de validación
  - Política de certificación
- Marco legal
- Glosario
- Atención al Ciudadano
- Preguntas más frecuentes
- Recursos
- PASAPORTE

POLICÍA NACIONAL

sede electrónica

Renovación Certificados

Renovación de claves sin renovación del soporte físico (tarjeta):

La renovación de las claves es voluntaria, gratuita y por iniciativa del ciudadano.

En fechas próximas a la caducidad de sus certificados, recibirá, en la cuenta de correo electrón momento de la expedición de su DNI, un aviso procedente de la dirección oficial notificaciones@polic caducidad de sus certificados electrónicos.

El titular puede proceder a renovar los certificados, si el estado de los mismos es uno de los siguiente

- Si fueron revocados a petición del ciudadano (solo podrá revocarse el certificado de firma digital)
- Por caducidad. Los certificados caducan pasados 60 meses desde la emisión de los mismos o s inferior a esos 60 meses, limitación a la fecha de caducidad del mismo (mejora de notoria impo los limitaba a 30 meses y solo se podían renovar una vez caducados o dentro de los 30 días de la fecha de caducidad.
- Para proceder a la renovación deberá mediar la presencia física del titular en una Oficina de expedición. El ciudadano, haciendo uso de los Puntos de Actualización del DNIe 3.0 habilitados en dichas oficinas y previa autenticación mediante la tarjeta y las plantillas biométricas (impresiones dactilares) capturadas durante la expedición de la Tarjeta, podrá desencadenar de forma desatendida el proceso de renovación de sus certificados.

EL PROCESO DE RENOVACIÓN DE CERTIFICADOS EN EL PUNTO DE ACTUALIZACIÓN DEL DNI 3.0 ES EL SIGUIENTE:

- El titular tras introducir correctamente el PIN, accede a la pantalla de "información sobre el contenido de su DNI 3.0", en la parte inferior puede visualizar el estado de sus certificados. En su caso, en la parte izquierda aparece una casilla "renovar certificados". Si se selecciona "renovar certificados" solicita nuevamente el PIN y posteriormente la presentación de la huella dactilar. Si el resultado es positivo se procede a la renovación de los certificados; este proceso dura aproximadamente 3 minutos. Es importante, no retirar el documento del lector de tarjetas hasta la finalización del proceso, porque el DNIe 3.0 podría quedar inservible. Si no fuere posible obtener la impresión dactilar de alguno de los dedos, el ciudadano deberá solicitar la renovación en un puesto de expedición atendido por un funcionario.

https://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_1028&id_menu=%5B37%5D

Smart Card -- el caso del DNI-e

https://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_1028&id_menu=%5B37%5D

Claves criptográficas en el DNI-e

- Cualquier operación criptográfica que requiera el uso de una de las claves privadas debe ser ejecutada en el interior del chip
- Las claves públicas se envían, tras su generación en el acto de expedición del DNI-e, a la CA para su inclusión en los correspondientes certificados digitales
  - una vez emitidos los certificados, estos se incorporan a la tarjeta para ser empleados en operaciones posteriores
  - los certificados digitales pueden ser leídos para su proceso de forma externa al chip

Revocación - DNI-e

- En el ámbito del DNI-e se usa **OCSP** para las revocaciones
  - cuando una aplicación requiere el estado actual de un certificado, envía una petición OCSP (mediante HTTP), a la URL del servicio de validación
  - una vez recibida la petición, el *OCSP Responder* accede a las CRLs, y averigua si dicho certificado se encuentra ahí incluido
- En la PKI adoptada para el DNI-e se ha optado por asignar las funciones de **Autoridad de Validación** a entidades diferentes de la **Autoridad de Certificación**
  - con el fin de aislar la comprobación de la vigencia de un certificado
  - existen tres **Autoridades de Validación**:
    - **FNMT**
    - **Ministerio de Administraciones Públicas**
    - **Ministerio de Industria**

- El marco legal básico del DNI-e es el siguiente:
  - Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre, por la que se establece un marco comunitario para la firma electrónica
  - Ley 59/2003, de 19 de diciembre, de Firma Electrónica
  - Ley Orgánica 15/1999, de 13 de diciembre, de Protección de los Datos
  - Real Decreto 1553/2005, de 23 de diciembre, por el que se regula documento nacional de identidad y sus certificados de firma electrónica
  - Real Decreto 1720/2007, de 21 de diciembre, relacionado con la protección de datos de carácter personal
  - Real Decreto 1586/2009, de 16 de octubre, Real Decreto 869/2013, de 8 de noviembre, y Real Decreto 414/2015, de 29 de mayo, por los que se modifica el Real Decreto 1553/2005

MENÚ BUSCAR el Periódico INICIAR SESIÓN

SOCIEDAD CASTELLERS CIENCIA MEDIO AMBIENTE TIEMPO SANIDAD SUCESOS PRIMERA PLAN@ +PERSONAS

Desactivada la firma digital de los DNI electrónicos por un fallo de seguridad

La medida, que afecta a los expedidos desde abril del 2015, viene por un fallo en el chip del fabricante

El problema está en un protocolo de transacciones digitales que utilizan millones de máquinas

Carmen Jané
Barcelona - Jueves, 09/11/2017 | Actualizado el 10/11/2017 a las 18:00 CET

7

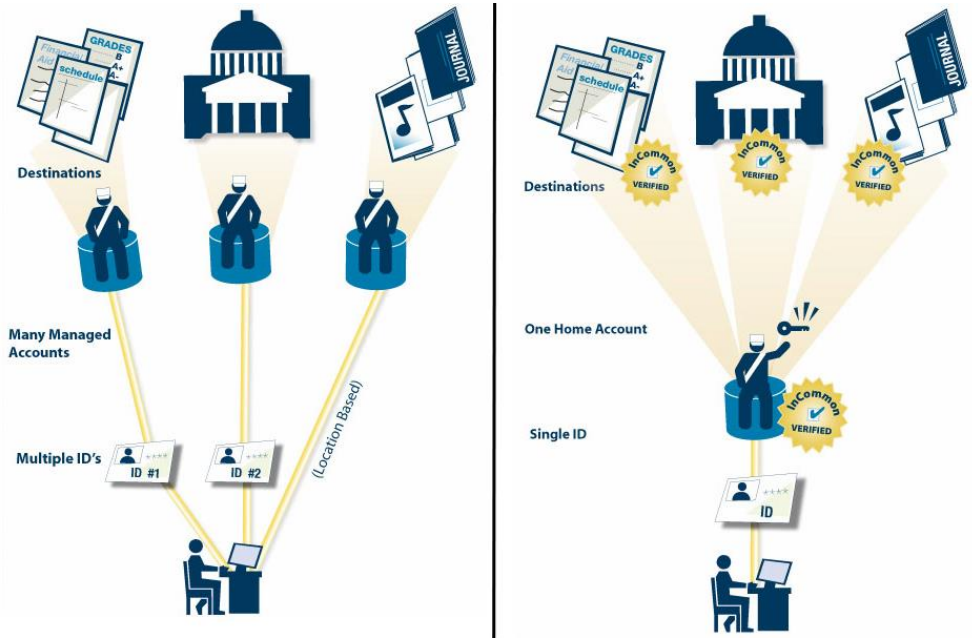
Un lector de DNI electrónico. / **PERIODICO**

http://www.elperiodico.com/es/sociedad/20171109/desactivada-la-firma-digital-de-los-dni-2015-posibles-fallos-de-seguridad-6412261

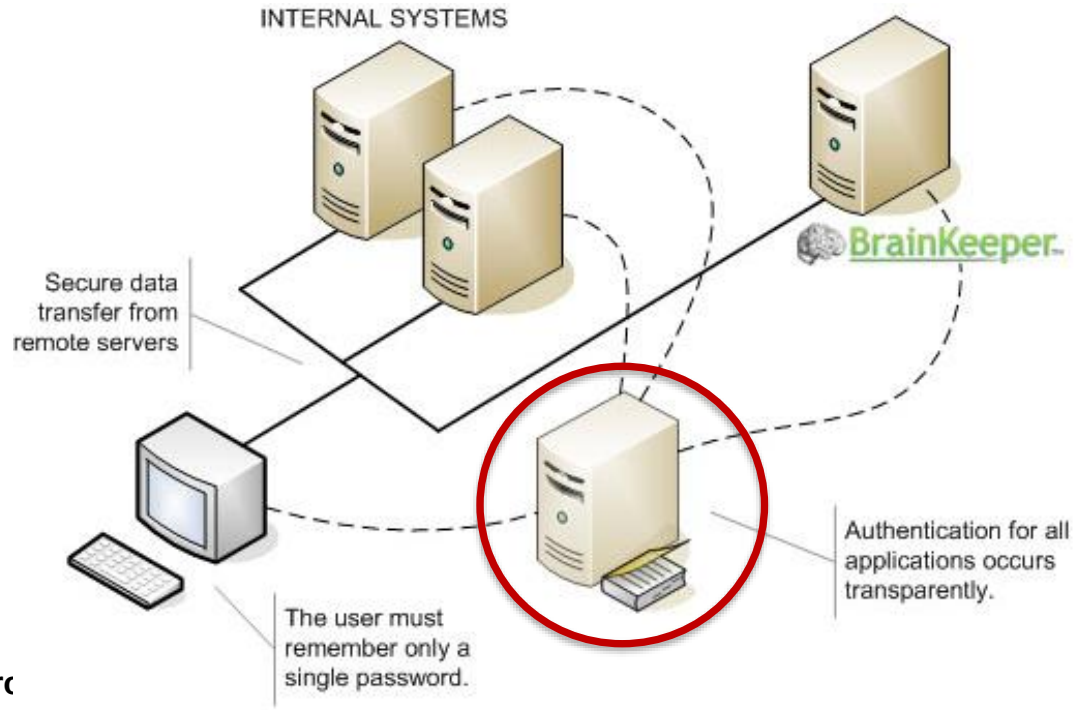
Mecanismo de Single Sign-On para Autenticación

Single Sign-On (SSO)

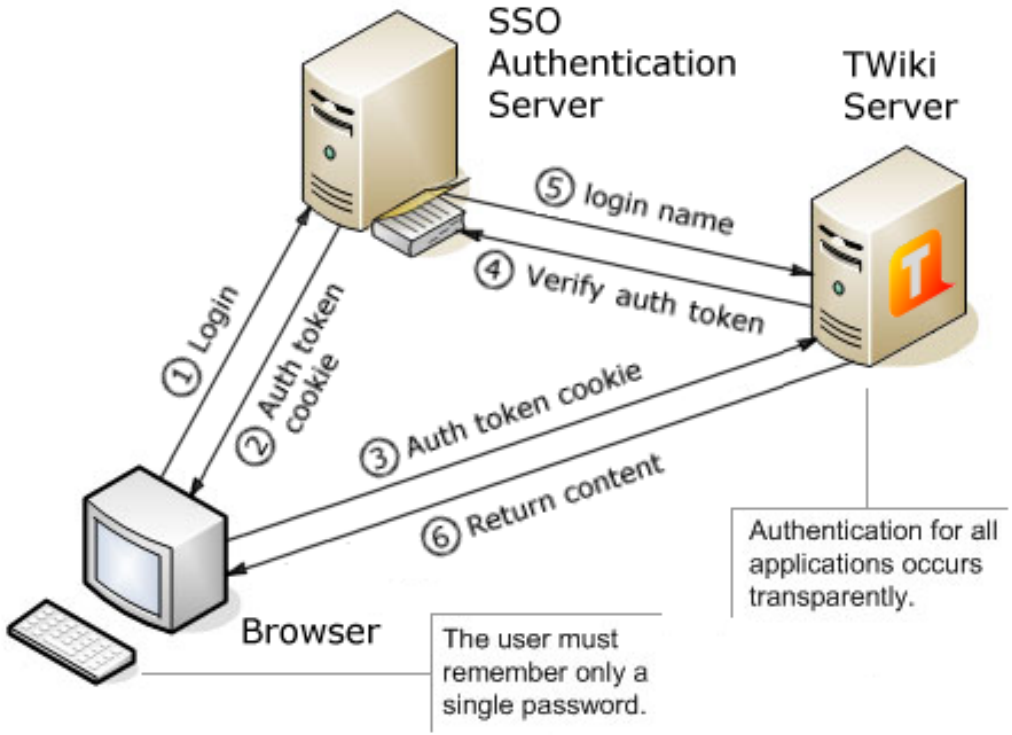
- El Single Sign-On es un mecanismo que permite a un usuario **autenticarse una sola vez** para acceder a todos los sistemas, independientes pero relacionados, a los que tiene acceso
- **Una vez autenticado, el usuario puede ir cambiando de un sistema a otro sin necesidad de autenticarse de nuevo**



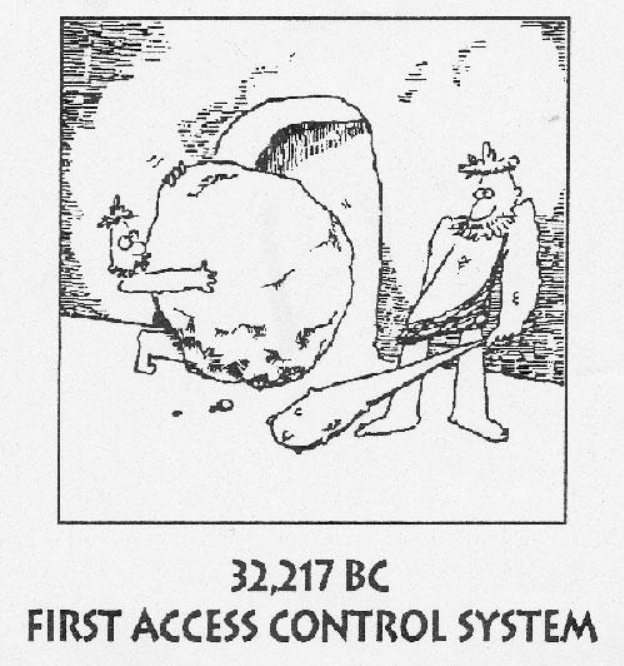
- Existen diferentes ventajas para el SSO:
  - **Usabilidad**: el usuario sólo ha de recordar un password, o usar un solo token, o un solo certificado, etc.
    - Reduce, por lo tanto, la probabilidad del error humano
  - **Seguridad**: reduce el riesgo de los ataques de intercepción
  - **Productividad**: reduce el tiempo de autenticación



- No obstante, también tiene la **desventaja** de que hay un **único punto de ataques**, el servidor SSO
  - Además, el intruso podrá entrar en todos los sistemas si su ataque tiene éxito aunque sea una vez



MECANISMOS DE CONTROL DE ACCESO

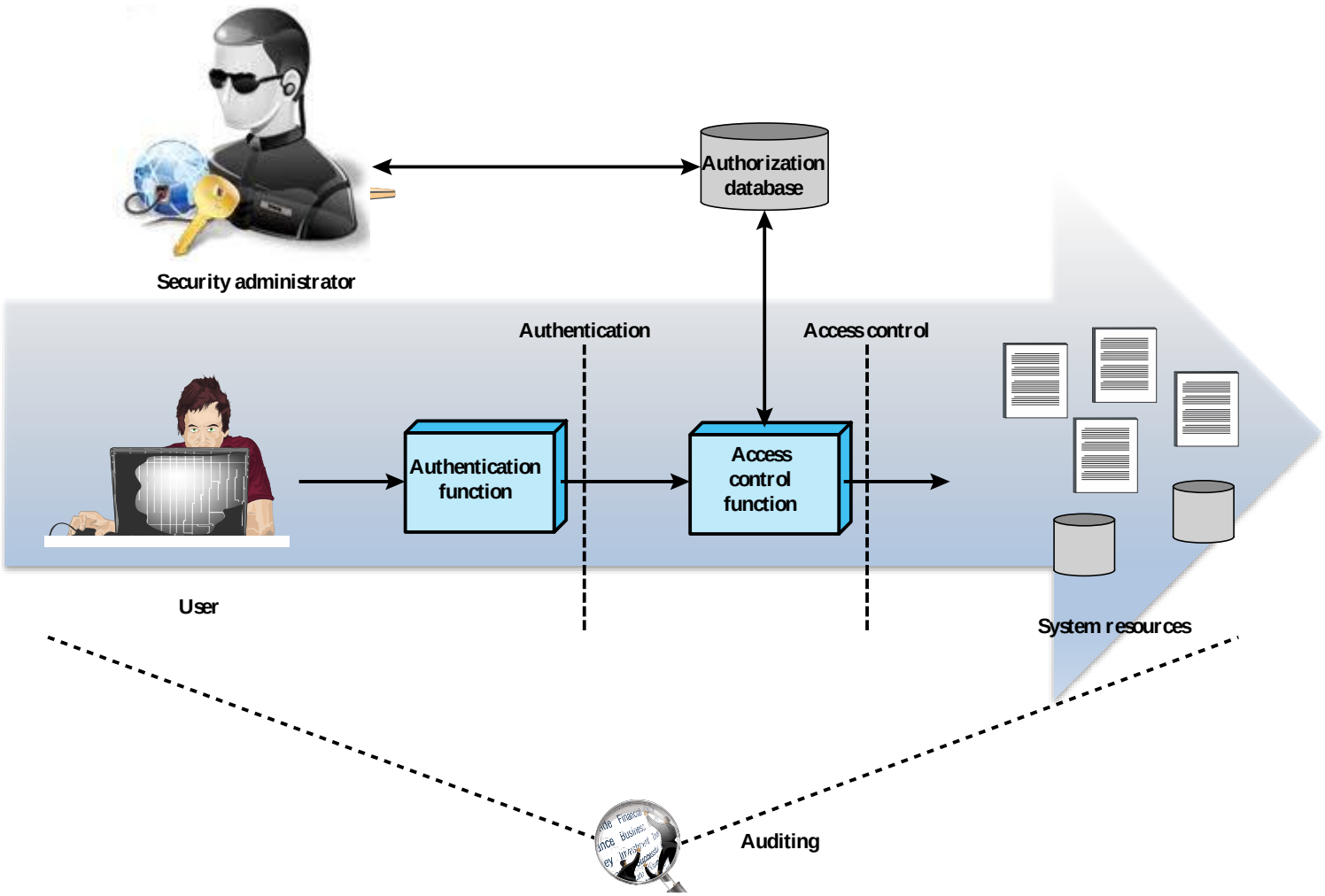


- El **control de acceso** es un elemento central – uno de los servicios esenciales – de la **Seguridad en Ordenadores**
- El RFC-2828 define la **Seguridad en Ordenadores** como:

  "measures that implement and assure security services in a computer system, particularly those that assure access control service"

- Los objetivos principales del control de acceso son:
  - prevenir los accesos a los recursos por parte de usuarios no autorizados
  - prevenir que los usuarios legítimos accedan a los recursos de forma no autorizada
  - permitir a los usuarios legítimos acceder a los recursos de una forma autorizada

- Por lo tanto, el control de acceso implementa una **política de control de acceso** que especifica:
  - **quién o qué** puede tener acceso a cada recurso del sistema
  - el **tipo de acceso** que se permite (cuándo, cómo, etc.)
- Existe una relación clara entre el control de acceso y otros servicios de seguridad, concretamente con los servicios de **autenticación, autorización y auditoría**
  - **Autorización**: concesión de un derecho o un permiso a una entidad para acceder a un recurso
  - **Auditoría**: revisión de los registros y actividades del sistema para:
    - garantizar el cumplimiento de la política establecida y los procedimientos operacionales
    - recomendar cambios en la política y en los procedimientos
    - comprobar la adecuación de los sistemas de control
    - detectar problemas de seguridad

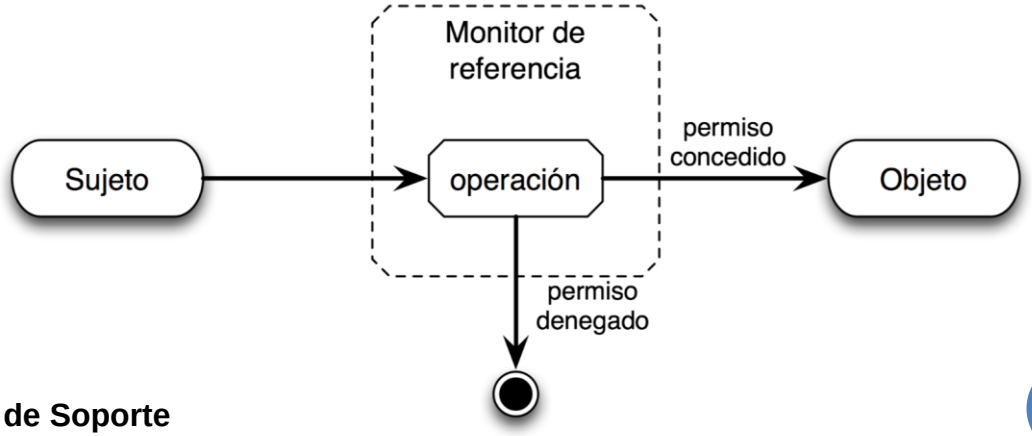

Security administrator
Authorization database
Authentication
Access control
Authentication function
Access control function
User
System resources
Auditing

- Como se puede observar en la figura anterior, el mecanismo de control de acceso hace de **mediador entre un usuario** (o un proceso) **y los recursos del sistema**:
  - Aplicaciones
  - Sistemas operativos
  - Firewalls
  - Routers
  - Ficheros
  - Bases de datos
  - Dispositivos concretos: servidores, sensores, dispositivos móviles, ….

Un mediador también es conocido como monitor de referencia

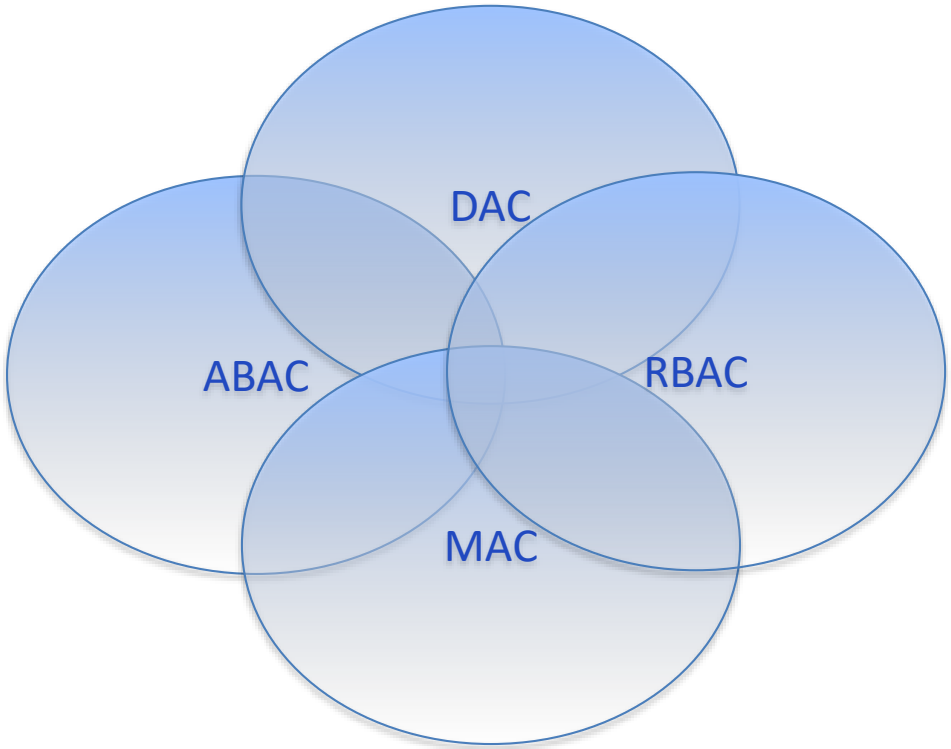
- La figura muestra un modelo simple de control de acceso, pero en la práctica puede haber **muchos componentes** que, de forma **cooperativa**, comparten la función de control de acceso

- Los elementos básicos de un control de acceso son:
  - **Objeto**: recurso al cual se controla el acceso
    - Ejemplos: registros, páginas, segmentos, ficheros, directorios, mailboxes, programas, procesadores, puertos de comunicación y nodos de red.
  - **Sujeto**: entidad que potencialmente accede a los objetos
    - generalmente el concepto de sujeto se asimila al concepto de **proceso**
      - de hecho, cualquier usuario o aplicación consigue el acceso a un objeto a través de un proceso que lo representa
  - **Derecho de acceso**: Describe la forma en que el sujeto podría acceder al objeto
    - read, write, execute, delete, create, …



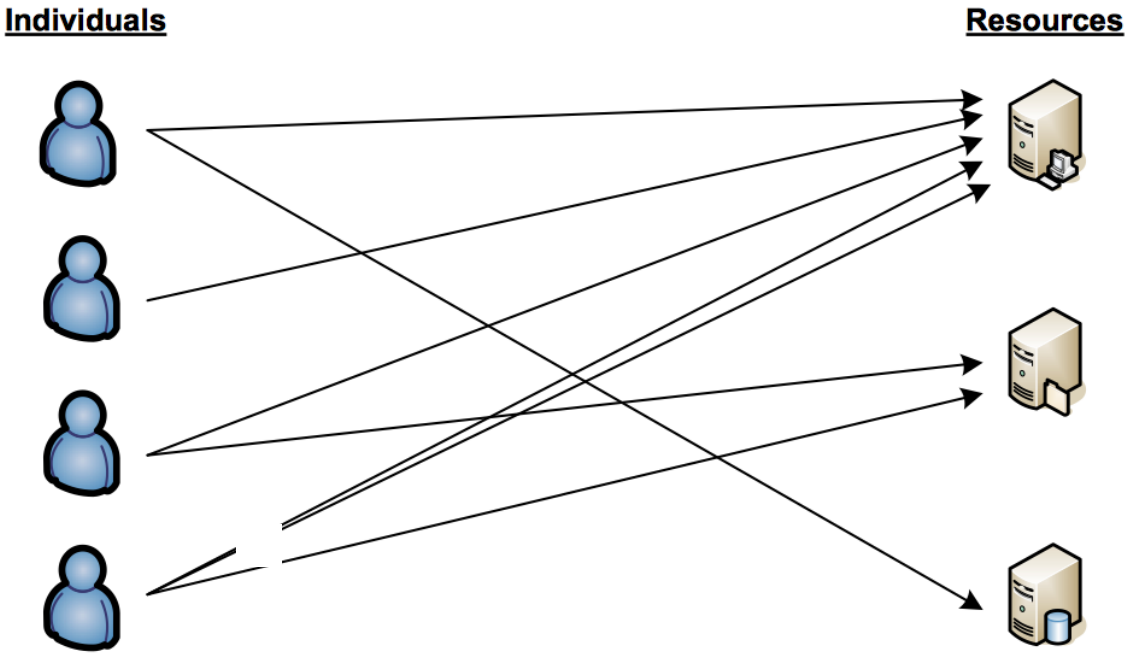
- Las esquemas de control de acceso se dividen principalmente en varias categorías:
  - **DAC (Discretionary Access Control)**: se basa en
    - **identidad del solicitante** y
    - **reglas de acceso** (que indican qué solicitantes están o no autorizados a hacer algo)
  - **MAC (Mandatory Access Control)**: se basa en comparar
    - **etiquetas de seguridad** (que indican la criticidad de los recursos) con
    - **autorizaciones de seguridad** (que indican las entidades que pueden acceder a ciertos recursos)
  - **RBAC (Role-based Access Control)**: se basa en
    - **rol** que tienen cada usuario dentro del sistema, y
    - **reglas** que indican qué accesos están permitidos a quien poseen un determinado rol
  - **ABAC (Attribute-Based Access Control)**: se base en
    - **Atributos** asociados con el usuario y que dependiendo del atributo se permite o no el acceso a un sistema
  - …

- Estas políticas no son mutuamente exclusivas
- De hecho, un mecanismo de control de acceso puede usar dos, tres o incluso todos los mecanismos para cubrir diferentes tipos de recursos del sistema



DAC (Discretionary Access Control)

- Como se ha comentado, DAC se basa en la identidad del solicitante y en las reglas de acceso (autorizaciones) que indican qué solicitantes están o no autorizados a hacer algo



b) Discretionary Access Control Using Access Control Lists

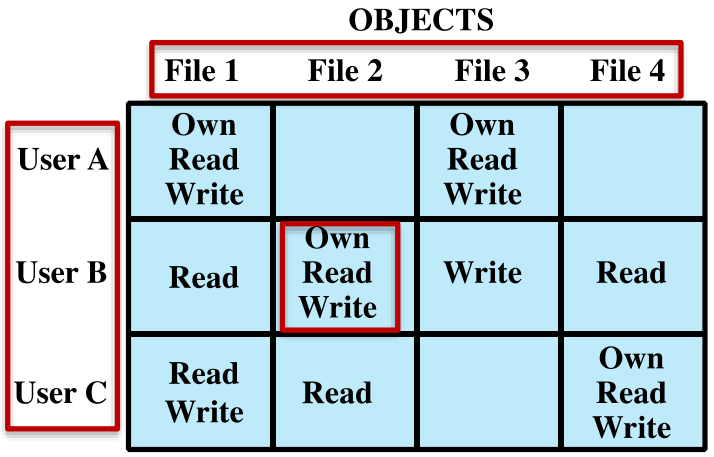
- La **matriz de acceso** es una solución general para DAC, tal y como ocurre en los S.O. y en los sistemas de administración de B.D.
- Una dimensión de esa matriz está formada por los sujetos:

  usuarios individuales, grupos de usuarios, equipos de red, hosts, aplicaciones, etc.

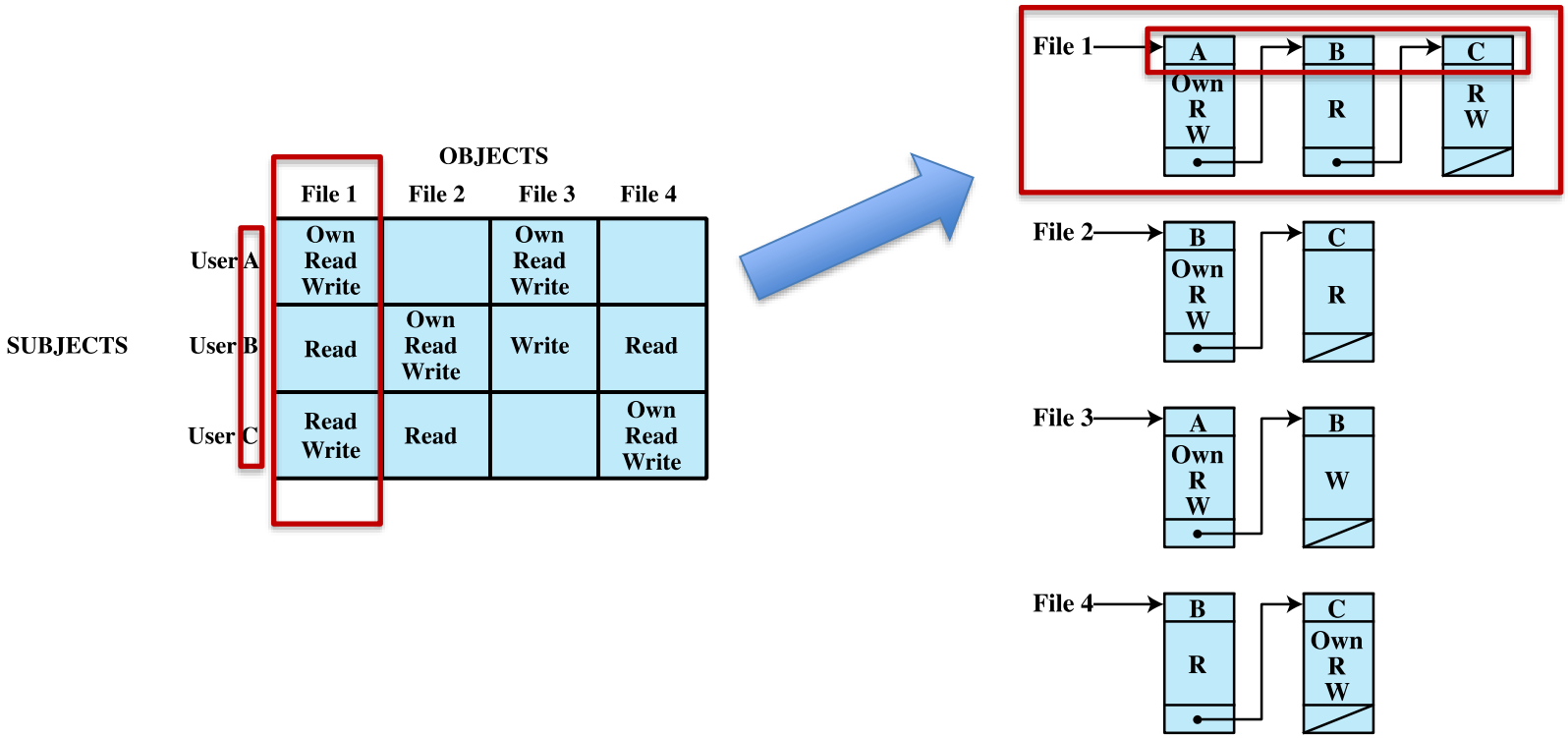
  que potencialmente acceden a los recursos
- La otra dimensión de la matriz está formada por los objetos:

  campos individuales de datos, registros, ficheros o una base de datos, etc.

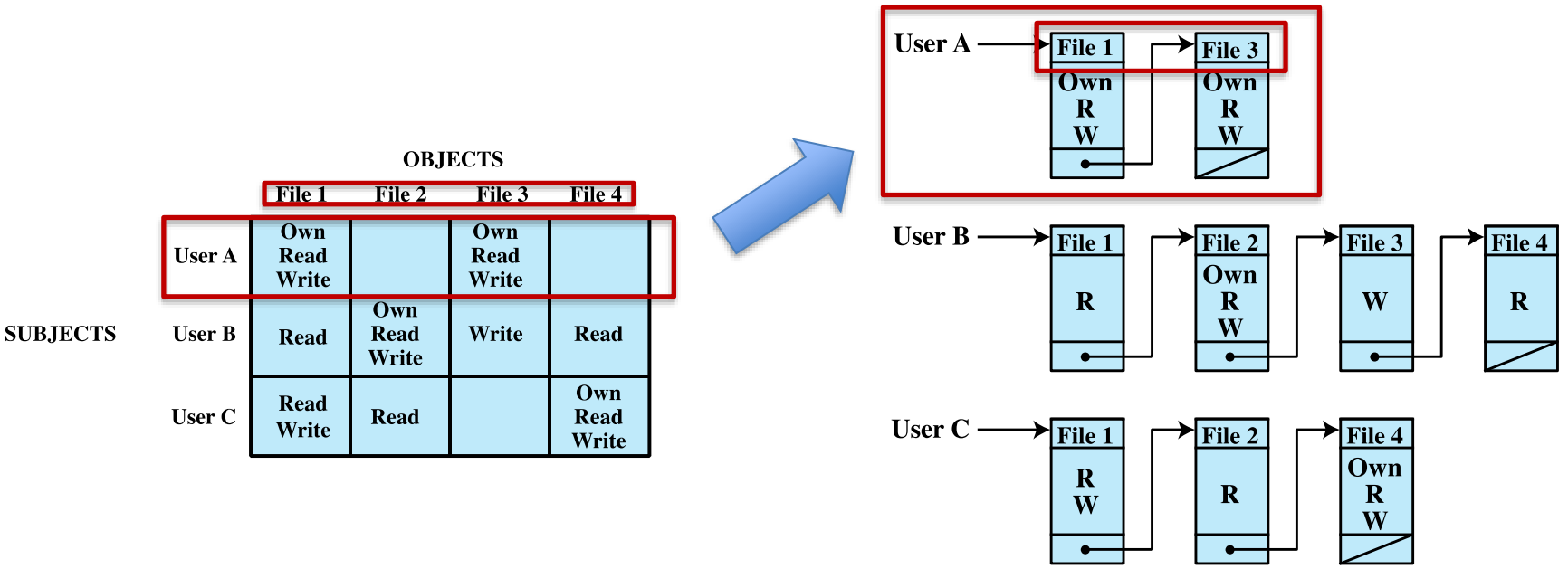
  que se podrían acceder
- Cada entrada en la matriz indica los derechos de acceso del sujeto para ese objeto



- En la práctica, una matriz de acceso se descompone en dos partes:
  - **Access Control List (ACL)**: es el resultado de la descomposición por columnas
    - por cada objeto, una ACL lista los usuarios y sus correspondientes derechos de acceso



– **Ticket de capacidades (o perfil de acceso)**: descomposición por filas; especifica los objetos autorizados y las operaciones para cada usuario



Dominio	Objeto	Derechos de Acceso
D1	A1	lec, eje
D2	A1	lec, esc, borr
	UC2	lec, esc, reb
D3	A2	lec, esc, eje
	A4	esc, lec, eje
	Imp1	imp
	UC2	lec, reb
D4	A3	esc
	Imp1	imp
	UC1	lec, esc
D5	A2	lec, eje
	A3	lec, eje
	Imp2	imp

- Ejemplo de lista de ACL:

$$L_{bar.txt} = \{\ (pepe, \{r\}),\ (paco, -),\ (luis, \{r, d\})\ \}$$
$$L_{foo.exe} = \{\ (pepe, -),\ (paco, \{x, d\}),\ (luis, \{x\})\ \}$$

- Ejemplo de lista de ACL:

$$L_{bar.txt} = \{ (pepe, \{r\}), (paco, -), (luis, \{r, d\}) \}$$
$$L_{foo.exe} = \{ (pepe, -), (paco, \{x, d\}), (luis, \{x\}) \}$$

- Ventajas:
  - Es fácil ver los permisos de acceso de un determinado objeto
  - Es fácil revocar todos los permisos sobre un objeto, poniendo $L_{ob} = \{\}$
  - Es fácil eliminar los permisos asociados a un objeto que ya no existe, por simplemente eliminar L_{ob}
- Desventajas:
  - Comprobar permisos de acceso de un determinado sujeto, usabilidad
- Uso:
  - Se suelen implementar en sistemas orientados a la gestión de recursos, como los S.O.

- Ejemplo de lista de capacidades / perfil de acceso:

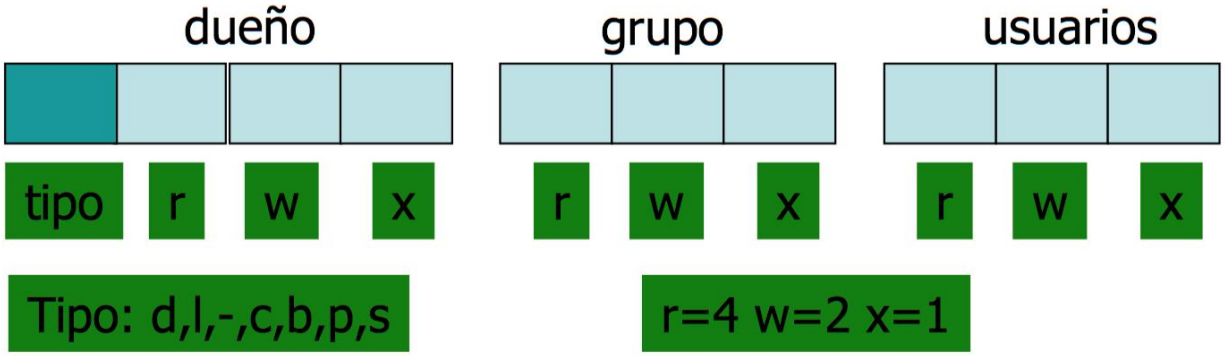
$$L_{pepe} = \{\ (bar.txt, \{r\}),\ (foo.exe, -)\ \}$$
$$L_{paco} = \{\ (bar.txt, -),\ (foo.exe, \{x, d\})\ \}$$
$$L_{luis} = \{\ (bar.txt, \{r, d\}),\ (foo.exe, \{x\})\ \}$$

- Ventajas:
  - Es fácil comprobar todos los permisos de un sujeto
  - Es fácil revocar todos los permisos de un sujeto, poniendo $L_{sj} = \{\}$
  - Es fácil eliminar los permisos asociados a un sujeto que ya no existe, eliminando L_{sj}
- Desventajas:
  - Comprobar los permisos de acceso sobre un determinado objeto, usabilidad
- Uso:
  - Se suelen implementar en sistemas orientados al usuario, como bases de datos o sistemas distribuidos

- **Tabla de Autorización**: Es una alternativa a la matriz de acceso. Contiene una fila por cada derecho de acceso de un sujeto a un recurso
  - es de uso más ágil en comparación con las ACLs o los tickets de capacidades

Subject	Access Mode	Object
A	Own	File 1
A	Read	File 1
A	Write	File 1
A	Own	File 3
A	Read	File 3
A	Write	File 3
B	Read	File 1
B	Own	File 2
B	Read	File 2
B	Write	File 2
B	Write	File 3
B	Read	File 4
C	Read	File 1
C	Write	File 1
C	Read	File 2
C	Own	File 4
C	Read	File 4
C	Write	File 4

- Ejemplo de permisos básicos en UNIX, usando DAC



192.168.234.139 - PuTTY

```
-rw-r----- 1 root shadow   928 Feb 14 08:23 shadow
-rw------- 1 root root     928 Feb 14 08:23 shadow-
-rw-r--r-- 1 root root     165 Feb 13 22:05 shells
drwxr-xr-x 2 root root    4096 Feb 13 22:05 skel
drwxr-xr-x 2 root root    4096 Mar  1 15:30 snmp
drwxr-xr-x 3 root root    4096 Feb 14 08:14 snort
drwxr-xr-x 2 root root    4096 Feb 13 23:06 ssh
drwxr-xr-x 4 root root    4096 Feb 15 14:44 ssl
-rw-r--r-- 1 root root    2082 Feb 24  2010 sysctl.conf
drwxr-xr-x 2 root root    4096 Feb 13 22:06 sysctl.d
drwxr-xr-x 2 root root    4096 Feb 13 22:05 terminfo
drwxr-xr-x 3 root root    4096 Feb 13 23:05 texmf
-rw-r--r-- 1 root root      21 Feb 13 22:06 timezone
-rw-r--r-- 1 root root    1260 May 30  2008 ucf.conf
drwxr-xr-x 4 root root    4096 Feb 13 22:06 udev
drwxr-xr-x 3 root root    4096 Feb 13 23:05 ufw
-rw-r--r-- 1 root root     274 Nov  4  2009 updatedb.conf
drwxr-xr-x 2 root root    4096 Feb 13 22:06 vim
drwxr-xr-x 2 root root    4096 Feb 13 23:06 w3m
drwxr-xr-x 2 root root    4096 Feb 24 11:07 webalizer
-rw-r--r-- 1 root root    4496 Sep  5  2010 wgetrc
drwxr-xr-x 3 root root    4096 Feb 13 22:06 X11
drwxr-xr-x 2 root root    4096 Feb 13 23:06 xml
root@debian6:/etc#
```