



UD2.1 – Configuració de Servidors Web Segurs

Desplegament d'Aplicacions Web
2on **DAW**

[ÍNDEX]

- MODELS D'AUTENTIFICACIÓ: BÀSICA I DIGEST
- CONFIGURACIÓ DESCENTRALITZADA
- PROTOCOL HTTPS
- CERTIFICATS I AUTORITATS DE CERTIFICACIÓ
- CONFIGURACIÓ **SSL/TLS** DE SERVIDOR: CERTIFICATS DE SERVIDOR

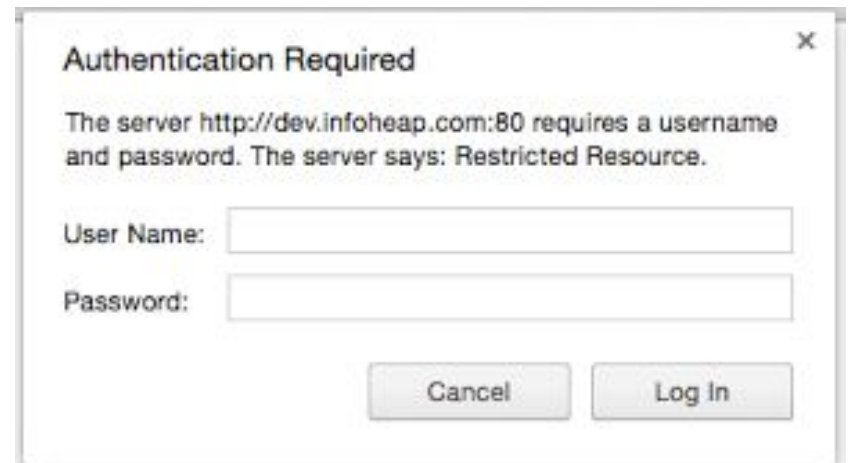
1. MODELS D'AUTENTIFICACIÓ: BÀSICA I DIGEST

- Els servidors web proporcionen mecanismes **d'autenticació**.
 - **L'autenticació**: verifica que algú és qui diu ser i es basa en un nom d'usuari i una contrasenya.
- Els usuaris i les seves contrasenyes es guarden en un magatzem o proveïdor d'autenticació, per exemple en un **fitxer** o una **base de dades**.



1. MODELS D'AUTENTIFICACIÓ: BÀSICA I DIGEST

- El **servidor web Apache** utilitza diferents mòduls per implementar aquests mecanismes de seguretat. Els podem veure a la documentació oficial:
<https://httpd.apache.org/docs/current/es/howto/auth.html>
- Aquests sistemes ens poden ser útils quan el nostre lloc web te **informació sensible** o **dirigida** només a un xicotet **grup de persones**.



1. MODELS D'AUTENTIFICACIÓ: BÀSICA I DIGEST

- **Model "basica":** no utilitza cap mecanisme criptogràfic per assegurar les dades, aqueste viatgen en clar **codificades en base64** dins les peticions HTTP.
- **Model Digest:** utilitza criptografia simètrica per xifrar les dades i assegurar la confidencialitat. Però no és del tot segur ja que hi ha un intercanvi previ de claus simètriques que es transmet en clar per la xarxa, per tant qualsevol pot interceptar-les per poder desxifrar posteriorment les dades.

Nota: Criptografia simètrica. La simetria està en què la clau de xifratge és la mateixa que la del procés invers: el desxifratge.

1. MODELS D'AUTENTIFICACIÓ: BÀSICA I DIGEST

- Model d'autenticació Bàsic:
 - Primer de tot necessitarem **crear un fitxer de contrasenyes**.
 - Aquest fitxer s'hauria de crear en un lloc que no fos accessible des de la web. Exemple:
 - */var/www/html/app1*
 - */var/www/passwd/app1/*
 - Per crear el fitxer de contrasenyes farem servir la utilitat que ve amb apache2 htpasswd que es troba al directori /usr/bin/ de la següent manera:
\$ htpasswd -c /var/www/passwd/passwords nomUsuari

Nota: Per afegir altres contrasenyes ho farem sense el paràmetre -c.

1. MODELS D'AUTENTIFICACIÓ: BÀSICA I DIGEST

Model d'autenticació Bàsic:

- El següent pas es configurar el servidor per a que sol·liciti una contrasenya i dir-li al servidor a quins usuaris se'ls permet l'accés
- Això ho farem en la pròpia configuració de cada vhost

1. MODELS D'AUTENTIFICACIÓ: BÀSICA I DIGEST

Model d'autenticació Bàsic:

/etc/sites-availables/001-es-example.conf

```
<VirtualHost *:80>
  ServerName www.example.com
  ServerAdmin webmaster@localhost
  DocumentRoot /var/www/html
  ...
  <Directory /var/www/html>
    AuthType Basic
    AuthName "Restricted Files"
    AuthUserFile /usr/local/apache2/passwd/passwords
    Require user nomUsuari
  </Directory>
</VirtualHost>
```



Directori al qual
s'aplicaran
les directives

1. MODELS D'AUTENTIFICACIÓ: BÀSICA I DIGEST

Directives

- **AuthType**: Selecciona el mètode que es va a fer servir per a autenticar l'usuari. El mètode més comú és **Basic**. (implementat al mòdul `mod_auth_basic`)
- **AuthName**: Compleix dues funcions importants:
 - Presenta aquesta informació a l'usuari com part del **quadre de diàleg** per introduir les credencials.
 - Establir **un domini** i poder determinar quina contrasenya enviar **per a cada zona restringida**.

1. MODELS D'AUTENTIFICACIÓ: BÀSICA I DIGEST

Directives

- **AuthUserFile** estableix la ruta al fitxer de contrasenyes que acabem de crear amb htpasswd. Si te un gran número d'usuaris, seria bastant lent buscar en un fitxer en text pla. Apache disposa de diferents "Auth Providers" per a emmagatzemar la informació de l'usuari en fitxers de bases de dades.

- **Proveedor de Autenticación**

- mod_authn_anon
- mod_authn_dbd
- mod_authn_dbm
- mod_authn_file
- mod_authnz_ldap
- mod_authn_socache

1. MODELS D'AUTENTIFICACIÓ: BÀSICA I DIGEST

Directives

- **Require** proporciona la part de la autorització del procés establint a l'usuari al que se li permet accedir a aquest àrea del servidor.
 - **Require user nom_usuari** : només amb el nom dels usuaris que poden accedir al recurs.
 - **Require group nom_grup** : només els usuaris que pertanyen al grup poden accedir al recurs.
 - **Require valid-user** : tots els usuaris vàlids poden accedir al recurs. Els usuaris vàlids són els que tindrem al fitxer de contrasenyes.

1. MODELS D'AUTENTIFICACIÓ: BÀSICA I DIGEST

- Model d'autenticació Digest:
 - Les credencials son intercanviades entre client i servidors de forma cifrada.
 - Primer de tot hem d'activar el mòdul **mod_auth_digest**.
 - En segon lloc crearem el fitxer de contrasenyes amb la instrucció:

***htdigest -c /usr/local/apache2/passwd/pass nomDomini
nomUsuari***

1. MODELS D'AUTENTIFICACIÓ: BÀSICA I DIGEST

Model d'autenticació Digest:

- El següent pas es configurar el servidor per a que sol·liciti una contrasenya i dir-li al servidor a quins usuaris se'ls permet l'accés.
- Això ho farem fent servir un fitxer **.htaccess**
- Aplicarem les **mateixes directives** que amb **basic**.

1. MODELS D'AUTENTIFICACIÓ: BÀSICA I DIGEST

Model d'autenticació Digest:

/etc/sites-availables/001-es-example.conf

```
<VirtualHost *:80>
  ServerName www.example.com
  ServerAdmin webmaster@localhost
  DocumentRoot /var/www/html
  ...
  <Directory /var/www/html>

    AuthType Digest

    AuthName "Restricted Files"

    AuthUserFile /usr/local/apache2/passwd/passwords

    Require user nomUsuari
  </Directory>
</VirtualHost>
```

1. MODELS D'AUTENTIFICACIÓ: BÀSICA I DIGEST

"Deurem tenir en compte que per a que la configuració aplicada siga segura deuria ser combinada amb un certificat ssl de forma que les credencials o la clau de xifrat no viatgen en pla en cap moment"



1. MODELS D'AUTENTIFICACIÓ: BÀSICA I DIGEST

Activitat 1. ¿Quan creus que podria ser útil aquesta funcionalitat?

2. CONFIGURACIÓ DESCENTRALITZADA

- No sempre els **desenvolupadors** o **clients** que comparteixen un mateix servidor poden tindre accés per a administrar-lo.
 - Servei d'allotjament.
 - Departament **de sistemes i desenvolupament**
- Es necessita algun mecanisme perquè cada **client** pugui gestionar la seua pròpia **configuració** sense que això implique la manipulació del servidor **HTTP**



2. CONFIGURACIÓ DESCENTRALITZADA

- El fitxer **.htaccess** ens permet realitzar configuracions distribuïdes del servidor web en lloc de **centralitzades** en un sol fitxer de configuració (**httpd.conf**).
 - Permet **modificar la configuració** principal **segons el directori** on se situa el fitxer **.htaccess**.
- Totes les directives de configuració s'apliquen al **directori** i **subdirectoris** on està situat el fitxer **.htaccess**.

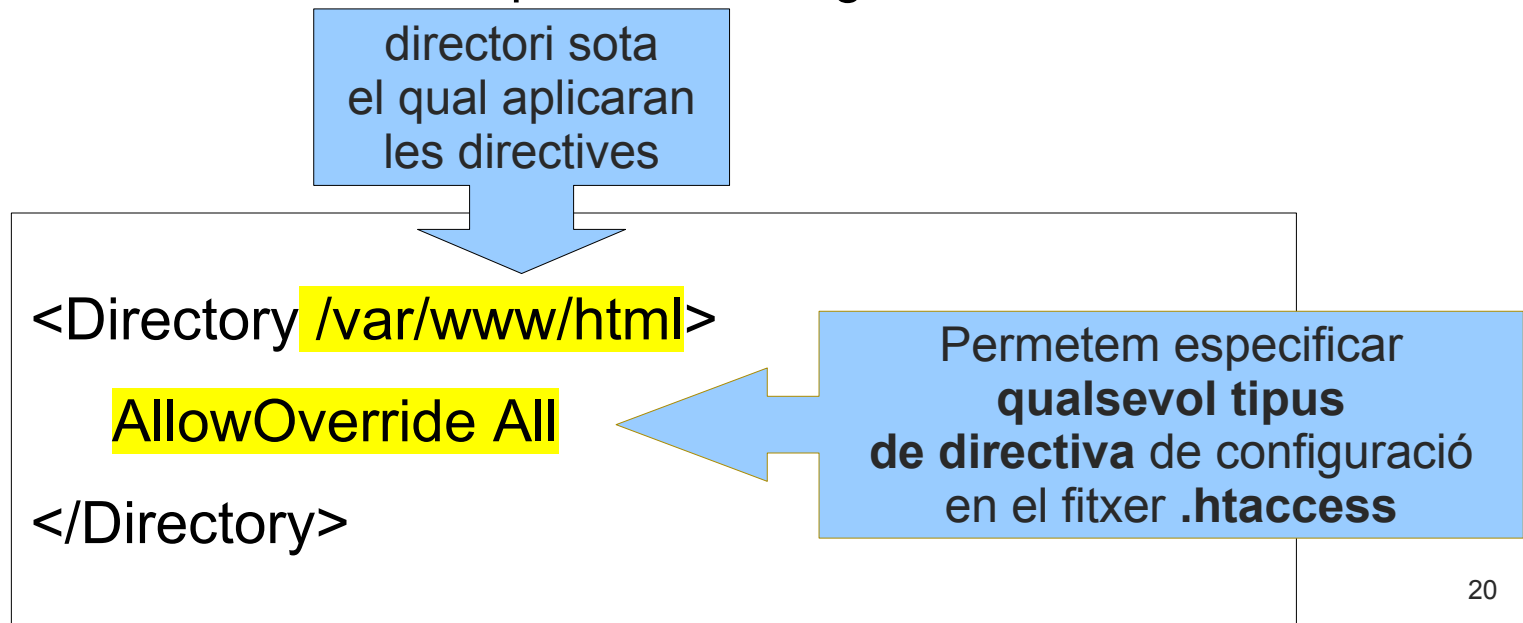


2.1 SOBRE-ESCRITURA DE CONFIGURACIÓ. FITXER .HTACCESS

- Aquest tipus de configuració distribuïda **només** s'hauria de realitzar quan es vol **compartir el servidor web** i **no es pot donar permís a tots els administradors** al fitxer de configuració principal.
- S'ha de tindre en compte que la utilització de fitxers **.htaccess** **disminueix el rendiment** del servidor i sempre que siga possible cal evitar-los.
- Per tal de evitar-los hem de dur a terme les configuracions en el **fitxer de configuració** de cada **host virtual** utilitzant la directiva **<Directory>**.

2.1 SOBRE-ESCRITURA DE CONFIGURACIÓ. FITXER .HTACCESS

- Per a poder **aplicar directives** en el fitxer `.htaccess` hem de permetre-ho en la configuració del vhost
 - Ho farem amb la directiva `AllowOverride` dins d'un tag `<Directory>` que **faça referència al directori** en el que volem permetre la sobre-escriptura de configuracions.



2.1 SOBRE-ESCRITURA DE CONFIGURACIÓ. FITXER .HTACCESS

- Les modalitats o opcions de la directiva AllowOverride son les següents:
 - **All:** permet utilitzar qualsevol directiva de configuració.
 - **None:** no permet utilitzar cap directiva de configuració.
 - **AuthConfig:** permet la utilització de directives d'autorització.
 - **FileInfo:** permet utilitzar directives per controlar els tipus de documents. (Error Document, Rewrite Rules,...)

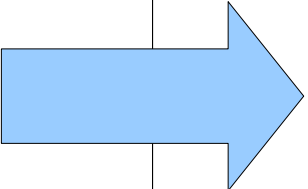
2.1 SOBRE-ESCRITURA DE CONFIGURACIÓ. FITXER .HTACCESS

- **Indexes:** permet utilitzar directives relacionades amb el llistat de directoris.
- **Limit:** permet utilitzar directives relacionades amb les llistes de control d'accés al servidor.
- **Options:** permet especificar directives relacionades amb característiques dels directoris.

2.1 SOBRE-ESCRITURA DE CONFIGURACIÓ. FITXER .HTACCESS

■ Configuració en virtualHost vs .htacceess

<i>/etc/sites_available/example.conf</i>	<i>/var/www/html/.htaccess</i>
<pre><VirtualHost *:80> ServerName www.example.com ServerAdmin webmaster@localhost DocumentRoot /var/www/html ... <Directory /var/www/html> Directiva 1; Directiva 2; Directiva 3; </Directory> </VirtualHost></pre>	<pre>Directiva 1; Directiva 2; Directiva 3;</pre>



2.1 SOBRE-ESCRITURA DE CONFIGURACIÓ. FITXER .HTACCESS

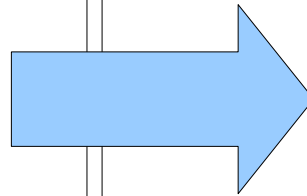
■ Exemple configuració autenticació

/etc/sites_available/example.conf

```
<VirtualHost *:80>
    ServerName www.example.com
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html
    ...
    <Directory /var/www/html>
        AllowOverride All
    </Directory>
</VirtualHost>
```

/var/www/html/.htaccess

```
AuthType Basic
AuthName "Restricted Files"
AuthUserFile /usr/local/apache2/passwd/passwords
Require user nomUsuari
```



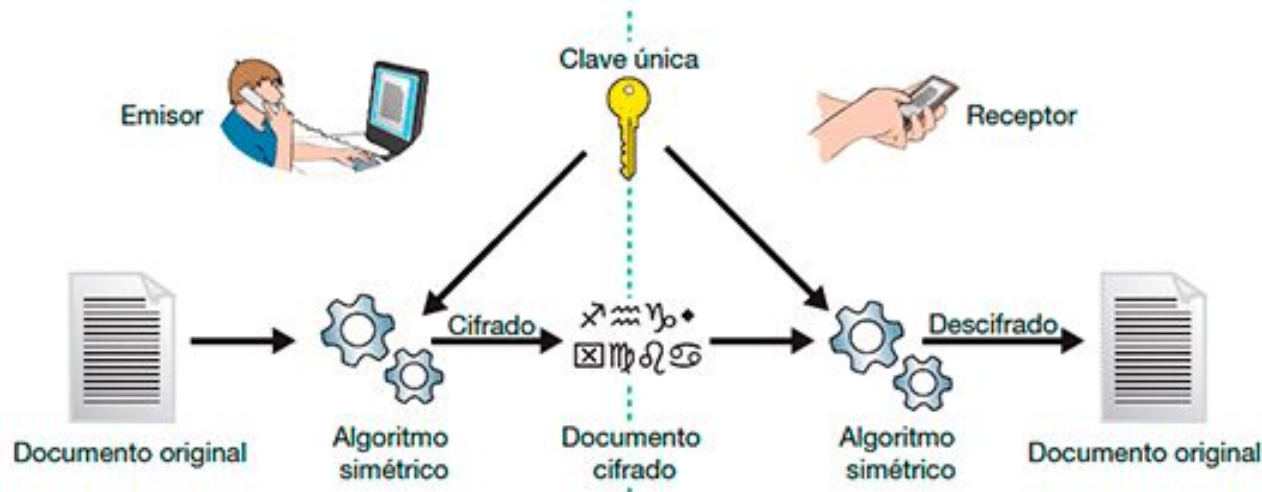
3. PROTOCOL HTTPS. CONCEPTES PREVIS

¿Què és la Criptografia?

- Tècnica utilitzada per a **convertir un text clar** en un altre **igual a l'anterior** però que només pot ser llegit per persones autoritzades.
- **SSL** utilitza **diversos algorismes** d'encryptació i autenticació.
 - Per a **establir la connexió** amb la màquina remota utilitza algorismes d'encryptació asimètrica.
 - Per a **la transferència de dades** utilitza algorismes d'encryptació simètrica, que són més ràpids.

3.1 CRIPTOGRAFIA SIMÈTRICA

- Els algorismes de criptografia simètrica són els que utilitzen la mateixa clau tant per al procés de **xifrat** com per al **desxifrat** del missatge.
- Els més utilitzats: **DONES, 3DES, AES, IDEA i Blowfish**



Problema:
Intercanvi
de claves

[3.1 CRIPTOGRAFIA ASIMÈTRICA]

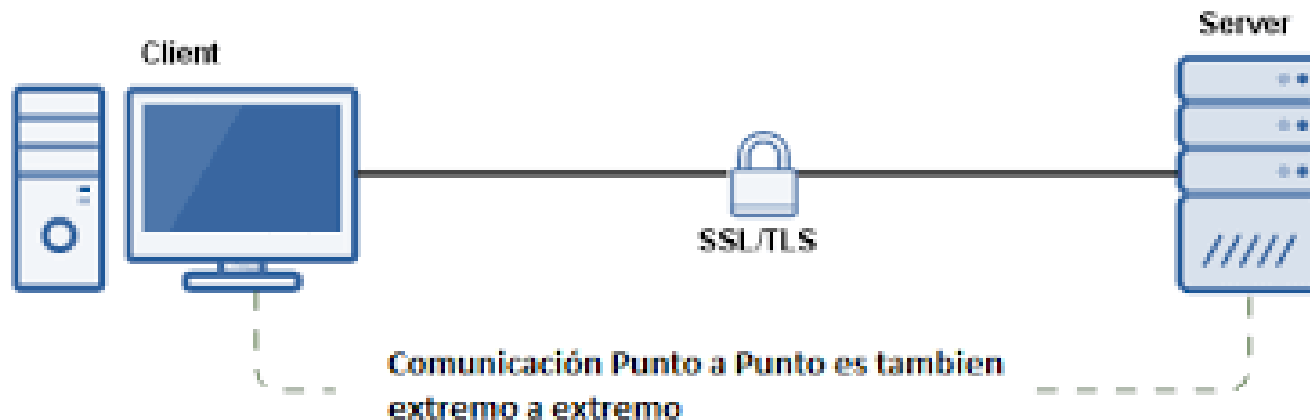
- Utilitza **2 claus matemàticament relacionades** de manera que el que **xifrem amb una** (clau pública) només pot **desxifrar-se amb la segona** (clau privada).
- Alguns algorismes representatius són: RSA, i *DSA



3.2 ¿QUÈ ÉS PROTOCOL HTTPS?

■ ¿Què és?

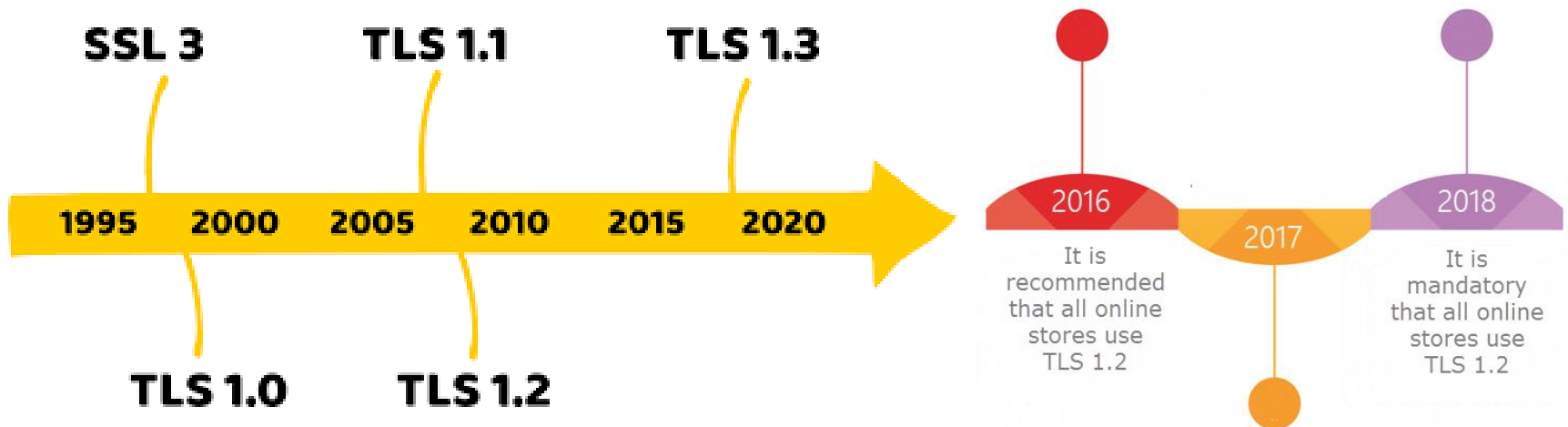
- El protocol **HTTPS** es basa en el **protocol HTTP** i afegeix xifrat SSL/TLS per assegurar les connexions entre emissor i receptor.
- **HTTPS = HTTP + SSL/TLS**
 - Utilitza per defecte **el port 443**



3.2 ¿QUÈ ÉS PROTOCOL HTTPS?

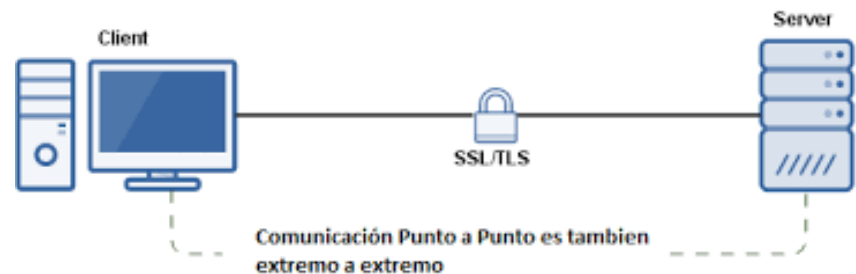
■ SSL/TLS

- Protocol segur que pertany a la capa de transport. Al llarg del temps s'han llançat diferents versions, la majoria de les quals són **vulnerables**



3.3 CARACTERÍSTIQUES

- El **protocol SSL/TLS** habilita les funcionalitats de **confidencialitat, integritat i autenticació** al protocol de nivell superior (**HTTP**) utilitzant mecanismes de criptografia tant simètrica com de clau pública.



3.3 CARACTERÍSTIQUES

- **Confidencialitat:** capacitat de garantir que la informació sols podrà ser accedida per aquells a qui va dirigida.
- **Integritat:** capacitat d'assegurar que les dades no seran modificades durant la transmissió.
- **Autenticació:** Garantir que l'interlocutor és qui diu ser.



3.4 FUNCIONAMENT

■ Exemple petició



3.4 FUNCIONAMENT

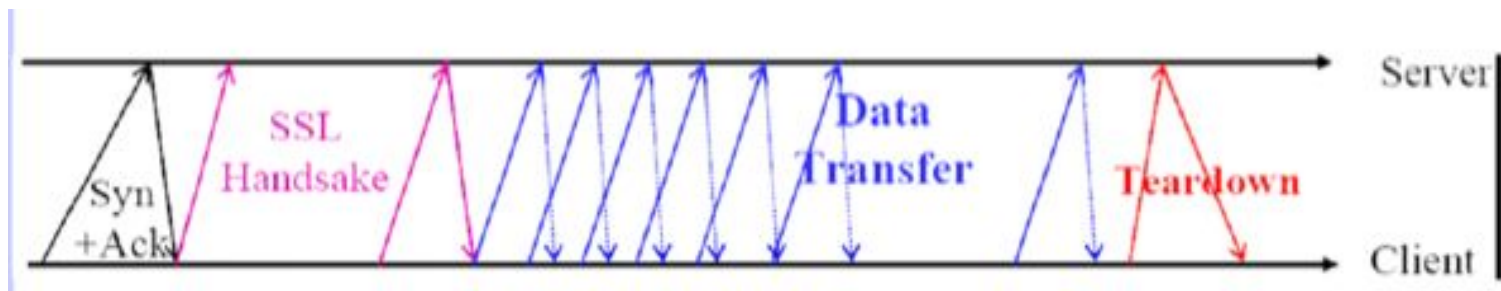
■ Confidencialitat

Protocol de Handshake

- Utilitza **criptografia de clau pública** per a establir una **clau compartida** entre client i servidor i es negocien els algorismes de xifrat i manteniment de la integritat que regiran la connexió.
 - El xifrat asimètric afecta al rendiment (**overhead**).

Protocol de transferència

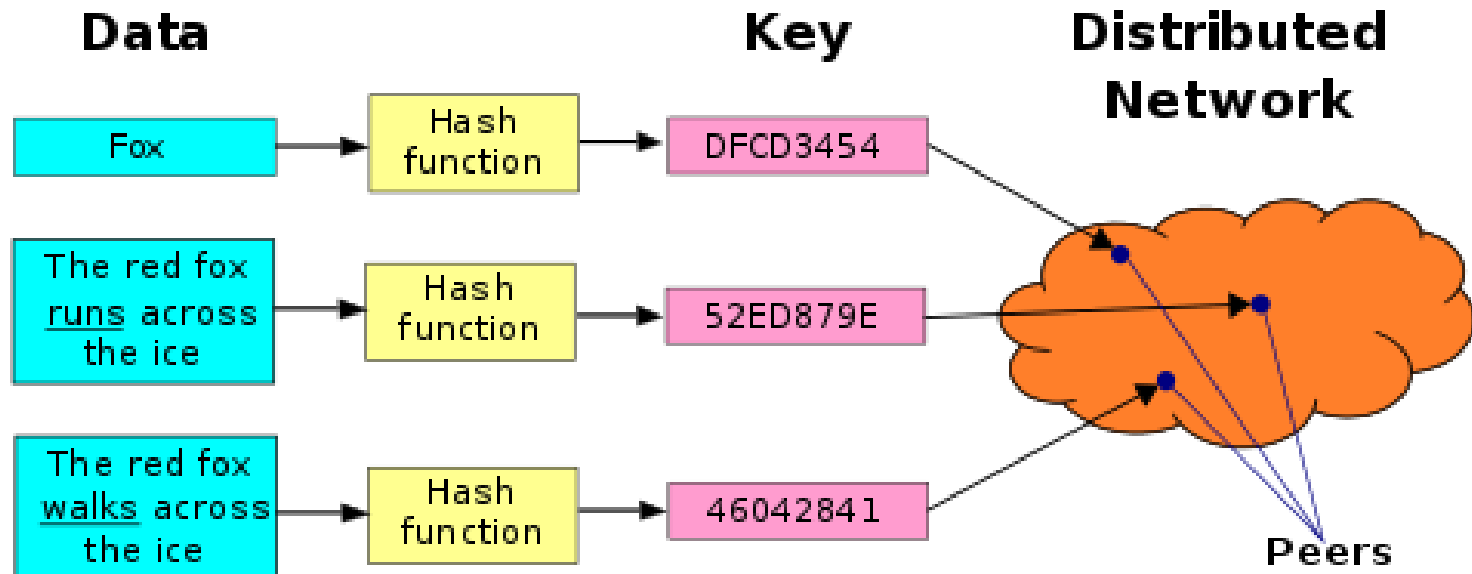
- Utilitza **la clau compartida establida en el punt anterior** per intercanviar dades entre client i servidor.



3.4 FUNCIONAMENT

■ Integritat

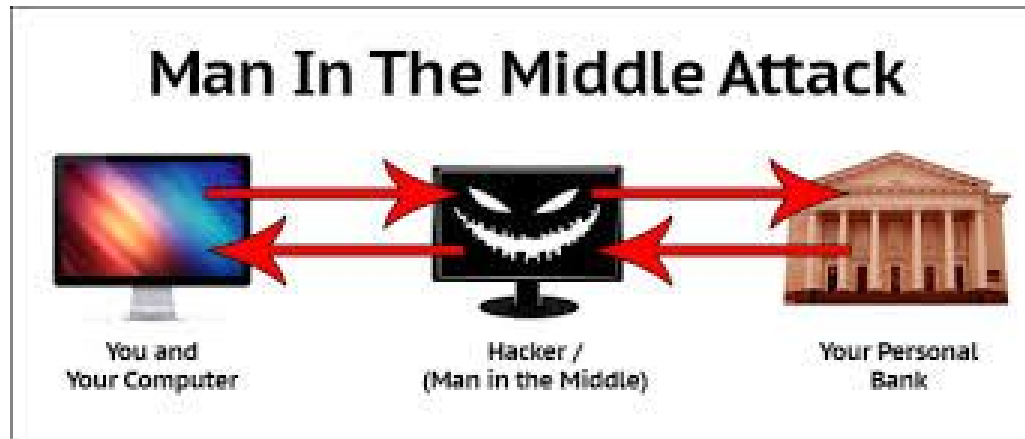
- TLS proporciona integritat dels missatges enviats mitjançant el **càlcul d'un resum o hash del missatge**. El algorisme es consensuat durant la fase de **handshake**



3.4 FUNCIONAMENT

■ Autenticació

*Fins ara hem xifrat les connexions però que passaria si un tercer intercepta la **primera comunicació** i es fa passar per nosaltres i per el banc...*



3.4 FUNCIONAMENT

■ Autenticació

- **Ana** utilitza la clau pública que pensa que és de Pepe per a xifrar el missatge.
- **Pepe** utilitza la clau pública que pensa que és de Ana.
- **Man** no sol accedeix a la informació sinó que pot modificar-la (Ex. transferir diners a un altre compte)

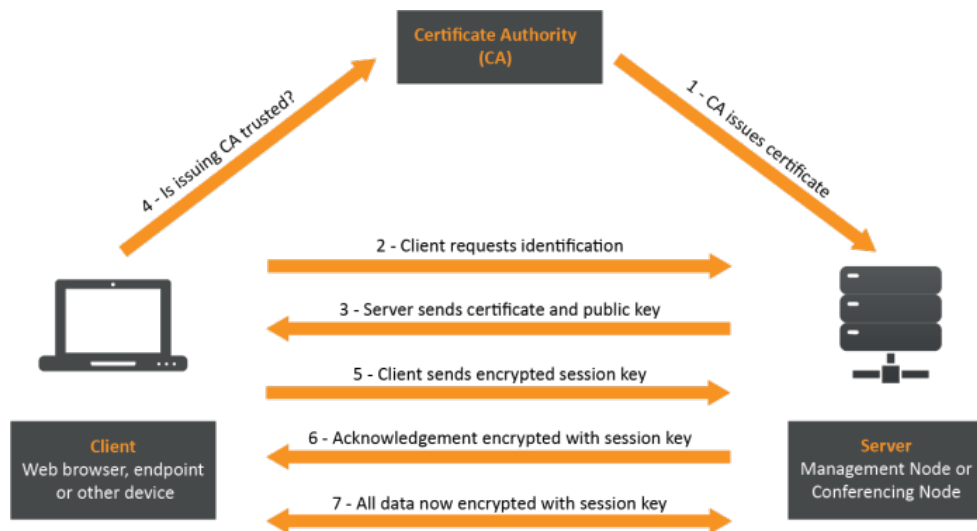


3.4 FUNCIONAMENT

■ Autenticació

- Solució: Certificats i autoritats de confiança
- Un tercer verifica l'autenticitat e identitat dels certificats i de la informació que contenen mitjançant la seua firma.

■ Chain of Trust → cadena de confiança

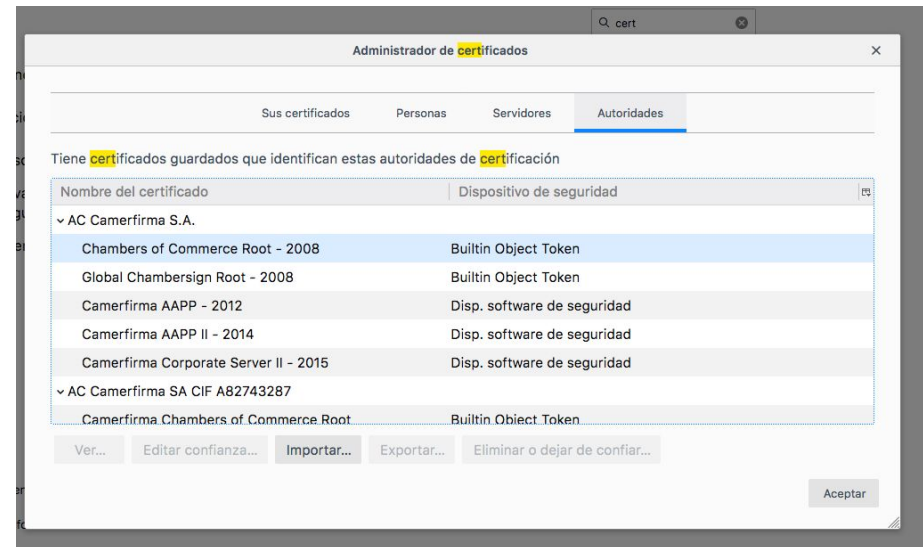
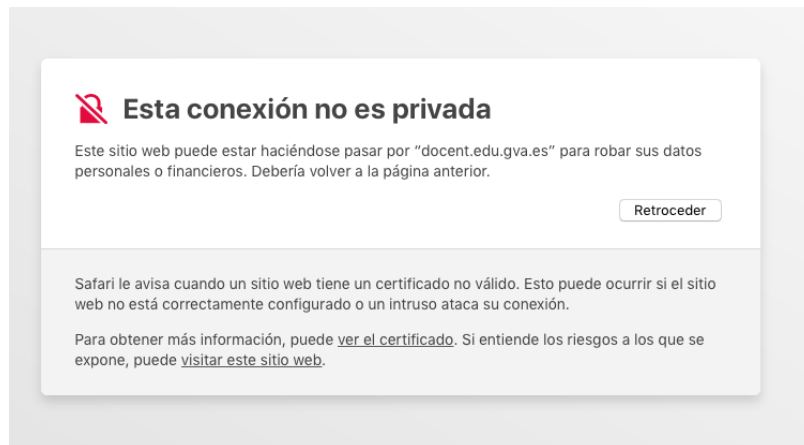


4. CERTIFICATS I AUTORITATS DE CERTIFICACIÓ

- **Autoritat certificadora (CA).** És tracta de una **tercera** entitat de confiança, responsable d'emetre i revocar certificats digitals.
- **Certificats:** recullen certes **dades** del seu **titular** i la seva **clau pública** i estan **signats** electrònicament per **l'Autoritat de Certificació** mitjançant la seva **clau privada**
 - Certifica que una clau pública pertany al seu propietari

4. CERTIFICATS I AUTORITATS DE CERTIFICACIÓ

- Els **clients disposen** de les **claus públiques** d'aquelles autoritats de certificació de les quals confien.
 - Qualsevol certificat que no haja sigut signat per una **CA** de confiança per al navegador, emetrà **un missatge d'error**.



4. CERTIFICATS I AUTORITATS DE CERTIFICACIÓ

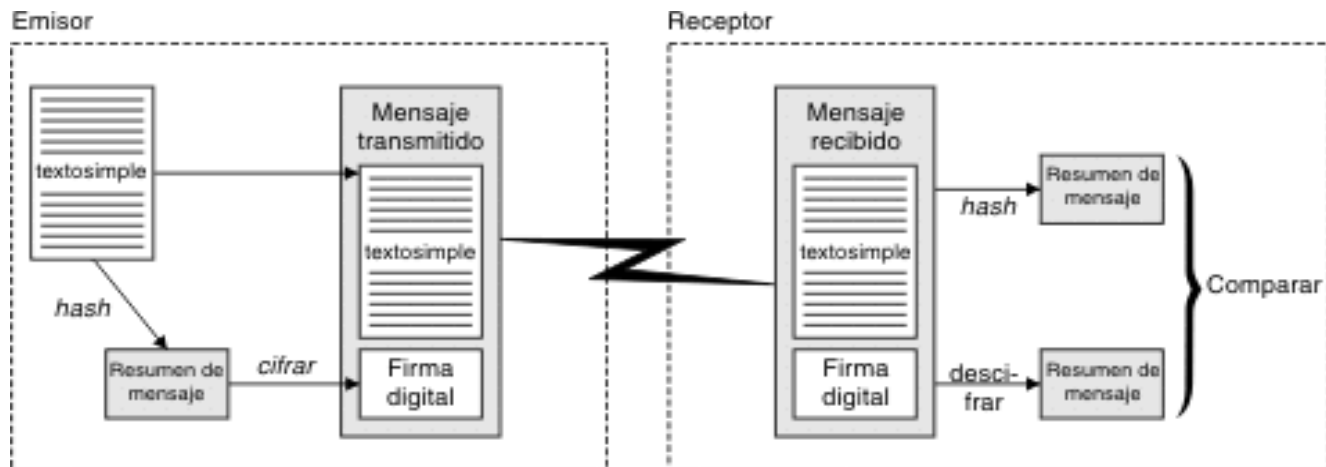
"The root certificates distributed with common browser software are added according to criteria defined by the browser supplier and vary from "pay us lots of cash"

"Els certificats arrel distribuïts als navegadors més comuns son afegits d'acord a criteris propis del creador, i poden variar d'acord a la quantitat que paguen"

4. CERTIFICATS I AUTORITATS DE CERTIFICACIÓ

■ Funcionament

- Si el navegador es capaç de "**desxifrar**" la signatura del missatge mitjançant la **clau pública** de la **CA** en la que confia i, a més aquesta coincideix amb el **hash** calculat a partir de la informació present en el certificat, haurà validat l'autoria del servidor.



4. CERTIFICATS I AUTORITATS DE CERTIFICACIÓ

■ Tipus de certificats

- **Validació del domini (DV):** Verifica sols si el domini està registrat a nom de qui va demanar el certificat. (nivell de seguretat baix).
- **Validació de la organització (VO):** S'investiga si la organització es propietària del domini. (nivell mitjà).
- **Validació estesa (VA):** Validació oficial de la entitat; registres oficials, us que es farà del domini,... (nivell alt)

4. CERTIFICATS I AUTORITATS DE CERTIFICACIÓ

■ Tipus de certificats



Validación del Dominio

Ventajas

- Se emite instantáneamente (menos de 10 minutos)
- Bajo costo, puesto que la validación es automática
- Cifrado básico
- Seguridad rápida y simple
- Garantía incluida

Desventajas

- Prueba sólo que su sitio es seguro (no su empresa)
- No otorga confianza a su negocio (ya que su negocio no está controlado)

Uso sugerido

- Solo para pruebas y uso interno
- Todas aquellas personas que necesitan un cifrado básico



Validación de la Organización

Ventajas

- Validación de sitio web y de su empresa
- Prueba que su negocio es legítimo y que usted es el propietario o está autorizado a ejecutarlo
- Verificación humana
- Licencia de servidor ilimitado
- Incluye sellos de sitio seguro

Desventajas

- La emisión del certificado puede requerir hasta dos días, si bien hacemos todo lo posible para emitirlo en el día
- Levemente más costoso del DV a causa de la investigación humana

Uso sugerido

- Sitios de comercio online
- Todas las personas que deseen demostrar que sus sitios y sus negocios son confiables



Validación Ampliada

Ventajas

- Activa la barra de direcciones verde
- Inspira los más altos niveles de confianza en sus clientes
- Protege su sitio contra el phishing
- Asegura los directores y demás personas interesadas de su empresa
- Procedimientos de investigación rigurosos

Desventajas

- Más caro
- Tómese hasta 5-10 días para publicar

Uso sugerido

- Sitios de comercio online
- Marcas nacionales y globales
- Todo negocio que desee impulsar sus ventas
- Toda persona que desee infundir más confianza a sus visitantes online
- Para una máxima protección contra el phishing

4. CERTIFICATS I AUTORITATS DE CERTIFICACIÓ

- **Autoritats de certificació de pagament**
 - Un criteri de selecció de l'autoritat es el **nivell de acceptació** que tenen els navegadors de ella.
 - Tots els navegadors disposen d'una llista de certificats acceptats.
 - **Cars i renovables** anualment



4. CERTIFICATS I AUTORITATS DE CERTIFICACIÓ

■ Certificats auto-firmats

- Si els nostres clients són interns podem ser nosaltres la nostra pròpia autoritat certificadora
 - Certificats auto-firmats
- Haurem d'instal·lar la clau pública als navegadors dels clients per a no tindre el missatge d'error corresponent



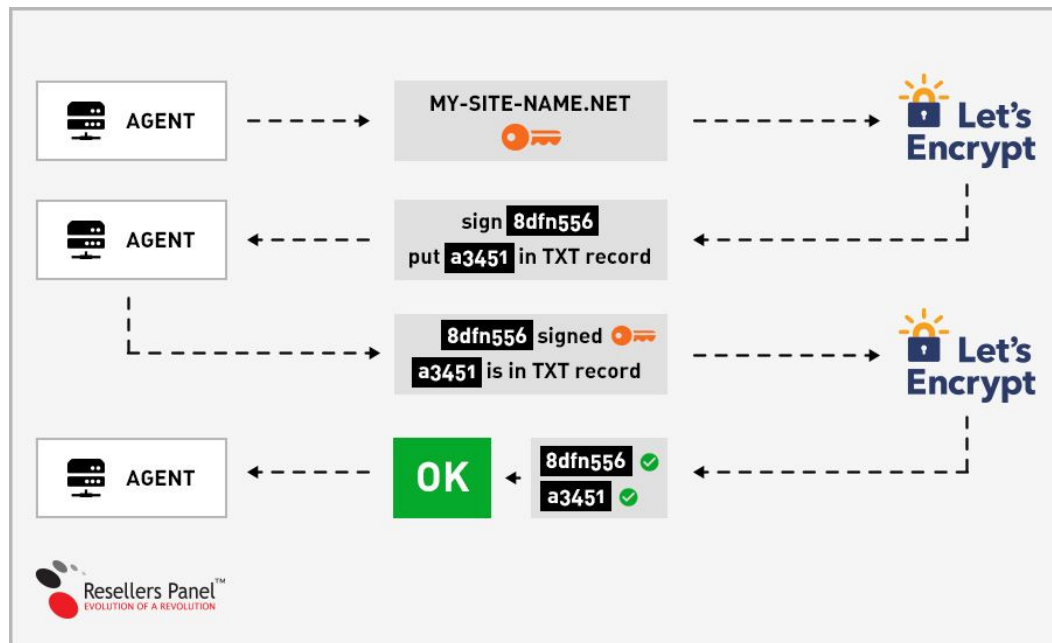
4. CERTIFICATS I AUTORITATS DE CERTIFICACIÓ

- **Let's encrypt**
 - **Autoritat de certificació gratuïta** promoguda per les principals companyies que ofereixen servicis mitjançant Internet.
 - **Acceptada** per la major part dels navegadors web com a "*autoritat de confiança*"
 - Proporciona 2 tipus de certificats
 - **SSL Individual**: per a un domini.
 - **SSL Wildcard**: per a domini i tots els seus subdominis.

4. CERTIFICATS I AUTORITATS DE CERTIFICACIÓ

■ Let's encrypt

- Renewable cada **90 dies**.
- El procés de renovació es automàtic mitjançant un script que s'executa al servidor.



[

]

- Això es tot... de moment :-)