Mobil- és webes szoftverek

Biztonság: HTTPS

Modern CSS layout megoldások: Flexbox

BME AUT
Automatizálási és
Alkalmazott
Informatikai Tanszék

Gincsai Gábor
gincsai@aut.bme.hu

HTTPS

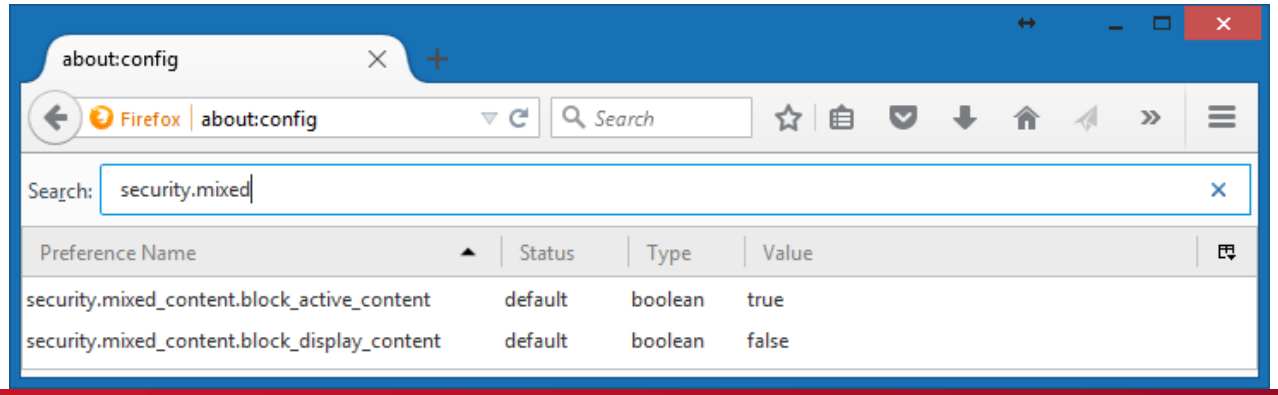
- A HTTP kapcsolat titkosítatlan
  - HTTP + SSL (Secure Sockets Layer protocol)
  - HTTP + TLS (Transport Layer Security)
- Nem önálló protokoll („HTTP over SSL”)
- Port: 443
- **https://** URI séma
- SSL/TLS felett más protokoll is mehet
  - Mivel alsóbb rétegben működik, mint a HTTP, ezért a hostname alapú virtual hosting megoldásokat nem támogatja.

Funkciók

- Szerver azonosítása (server authentication): pontosan kivel áll kapcsolatban a kliens.
  - Képes a kliens azonosítására (mutual authentication) is, de az általában nem használatos.
- Kommunikáció titkosítása (encryption): harmadik fél nem tudja lehallgatni (eavesdropping).
- Tartalom integritása (integrity): harmadik fél nem tudja megváltoztatni (tampering).

Funkciók

- Oldalon összes hivatkozásnak **https://**-nek kell lennie, különben: mixed content warning.
- Firefox 23: Mixed content blocker
  - Active content
    - script, stylesheet, frame - blocked by default
  - Passive (display) content
    - image, audio, video, object - not blocked
  - Nincs domain whitelist



Tanúsítvány (certificate)

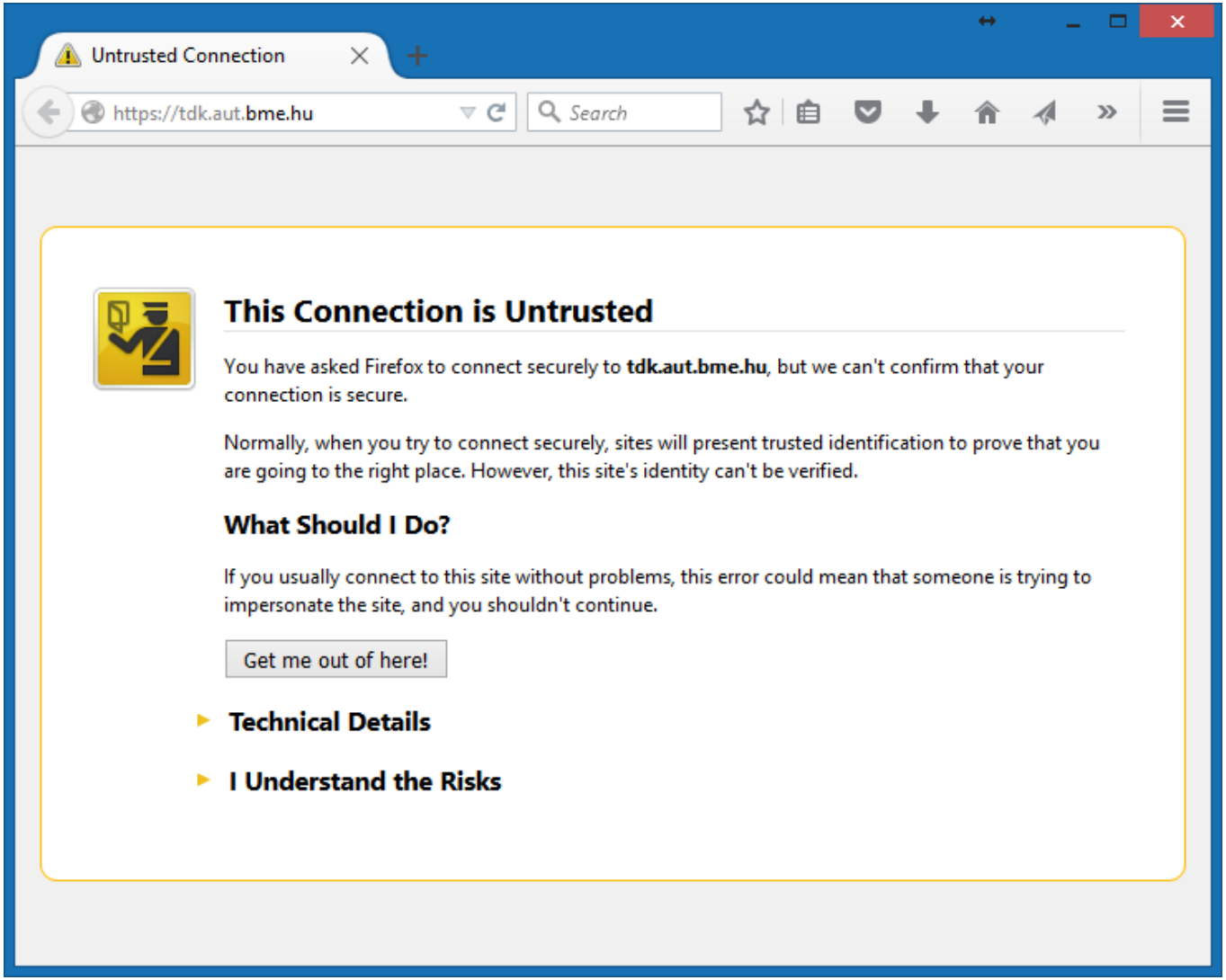
Alapelv: egy megbízható harmadik fél (trusted 3rd party) igazolja a szerver hitelességét.

- **Tanúsítvány (X.509 certificate)**
- **Tanúsítvány lánc (certificate chain, chain of trust)**
- **Certification Authority** (CA): tanúsítvány kiadó
  - Subordinate CA (intermediate CA)
  - Root Certification Authority (Root CA)

Önaláírt tanúsítvány (self-signed certificate)

- Előnyök:
  - Olcsó
  - Gyors
  - Tetszőlegesen testreszabható
- Hátrányok:
  - Nem azonosítja a szervert.
  - Man-in-the-middle támadással könnyen kijátszható, ezért nem ajánlott.
  - A felhasználókat arra tanítja, hogy elfogadják a nem hiteles tanúsítványt.

Tanúsítvány probléma



Tanúsítvány részei

- Version
- Serial Number
- Signature algorithm
- Signature
- **Issuer**
- **Valid from, Valid to**
- Subject
- Public key
- Thumbprint algorithm
- **Thumbprint (fingerprint)**
- Extensions (opcionális)
  - Key usage
  - Subject Alternative Name (SAN)

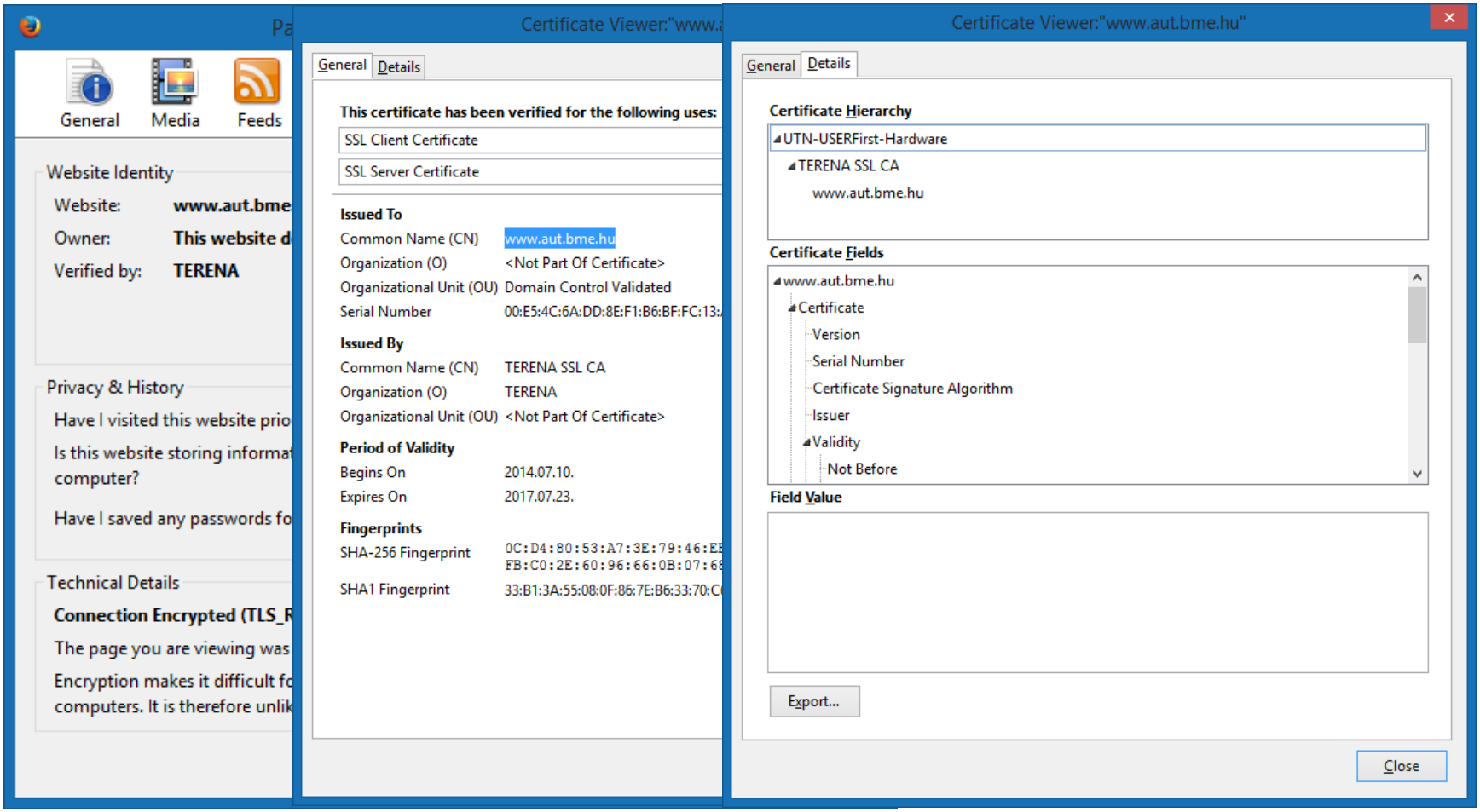
Tanúsítvány privát kulcsa

A privát kulcs nem része a tanúsítványnak.

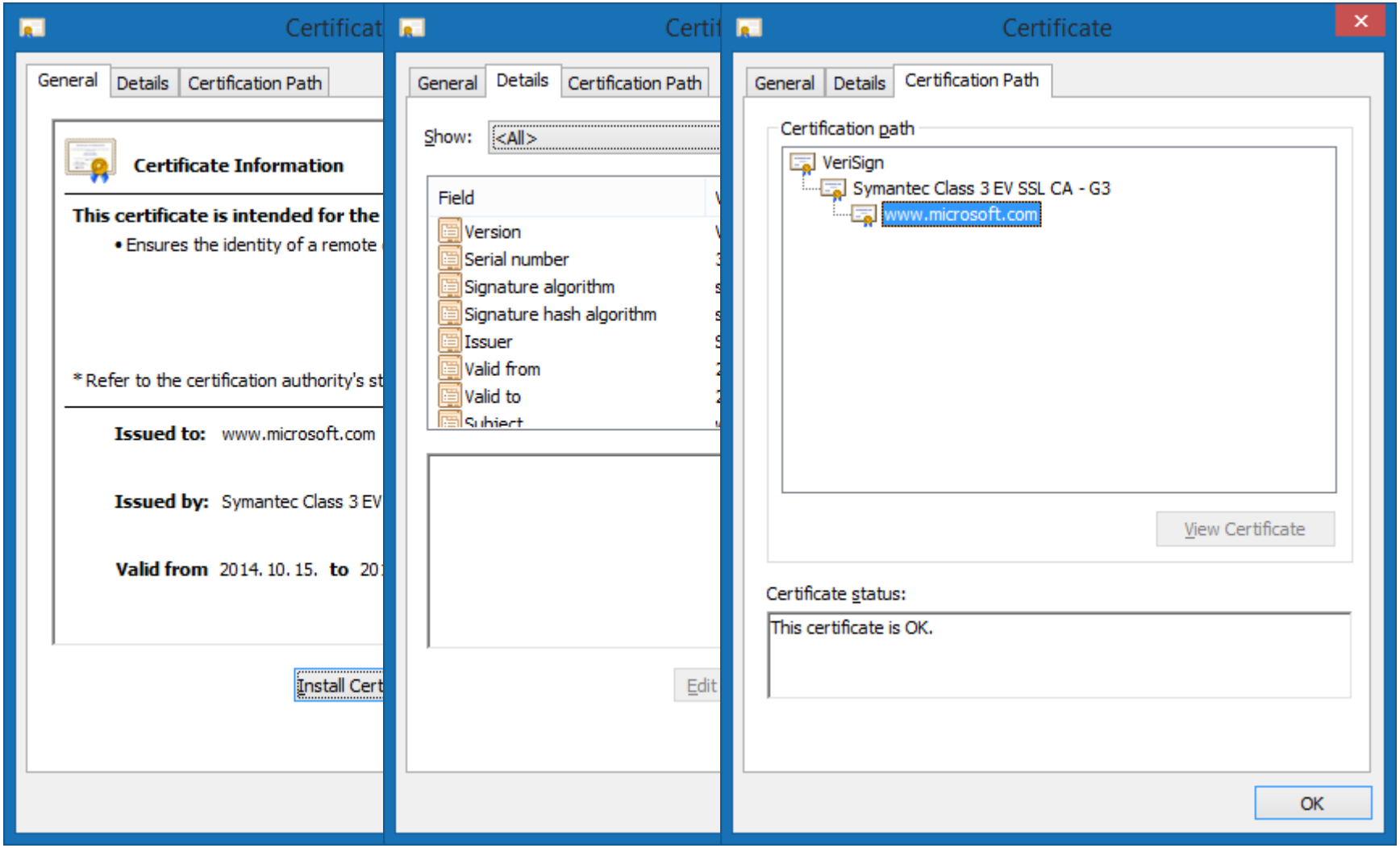
- Lehet jelszóval védett.
- Lehet exportálható vagy nem exportálható.
- A webszerveren keletkezik, nem jut el a CA-hoz. A CA csak azt igazolja, hogy a nyilvános kulcs az adott tulajdonosé.
- Fájl formátumok
  - .pem, .cer, .crt, .der, .p7b, .p7c, .p12, .pfx

AUT portál tanúsítványa Firefox

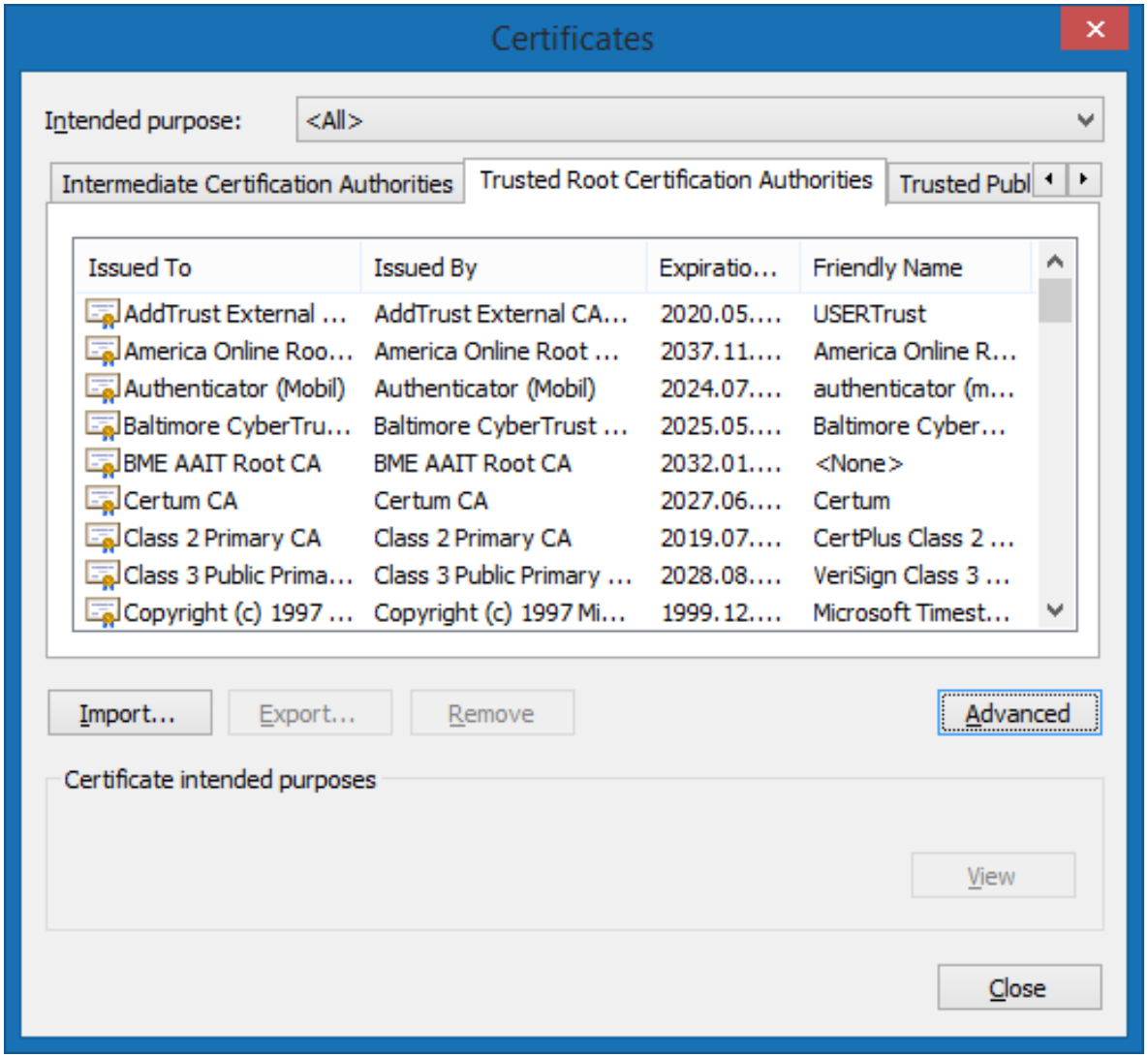
- https://www.aut.bme.hu



https://www.microsoft.com IE



IE Trusted Root certificate-k



A tanúsítvány ellenőrzése I.

Érvényes, ha mind a 4 feltétel teljesül:

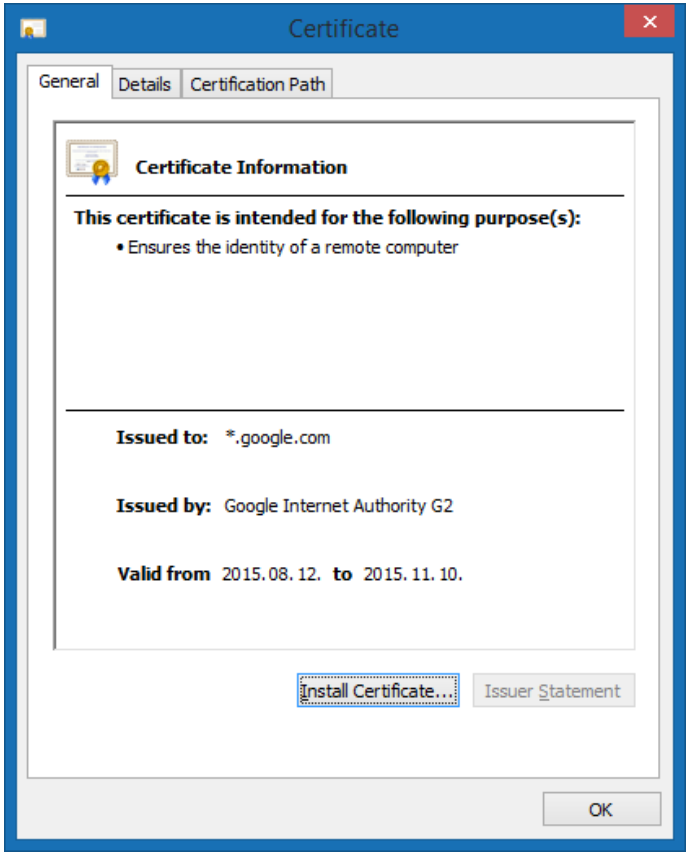
1. **A kiállító hiteles.**
   - A böngészőnek meg kell bíznia a CA lánc minden szereplőjében.
   - A gyökér tanúsítvány kiadónak szerepelnie kell a böngésző Trusted Root CAs listájában.
   - Az önaláírt tanúsítvány nem azonosítja a szervert, de titkosítja a kapcsolatot.
2. **Nem járt le.**
   - A tanúsítványok érvényességi ideje általában 1-3 év.

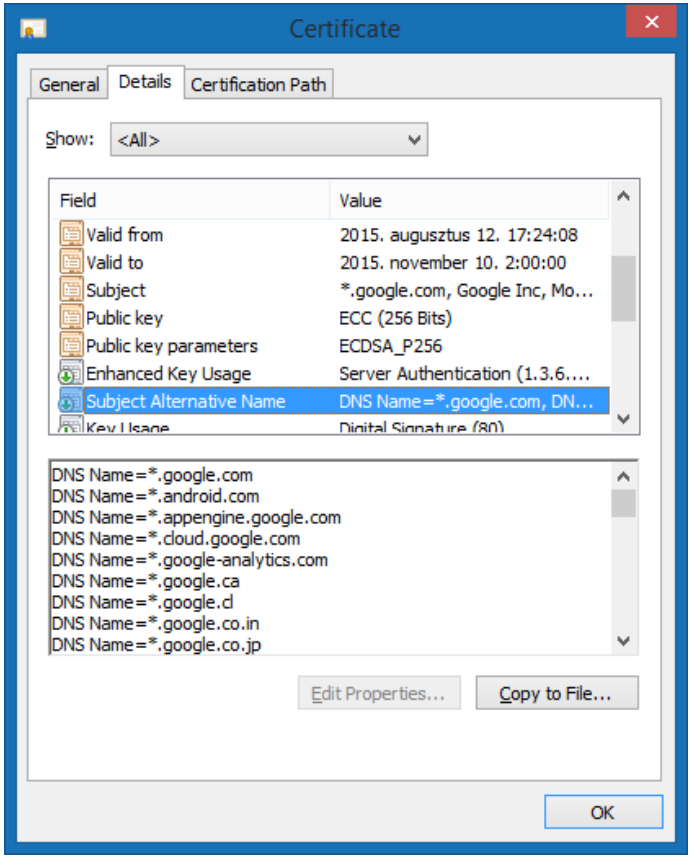
A tanúsítvány ellenőrzése

3. **Az aktuális szerver számára állították ki.**
   - A tanúsítvány Subject mezőjében lévő CN-nek meg kell egyeznie az oldal betöltéséhez használt FQDN-nel.
     - https://example.com != https://www.example.com
   - Ha több, alias FQDN is van, akkor át kell őket irányítani arra, amelyik a tanúsítványon szerepel.
   - Wildcard certificate: ***.example.com**
     - Több al-domainhez
     - Csak 1 szint mélységig
     - Extended Validation nem támogatja

https://www.google.com

- *.google.com
- Subject Alternative Name mezőben több név.



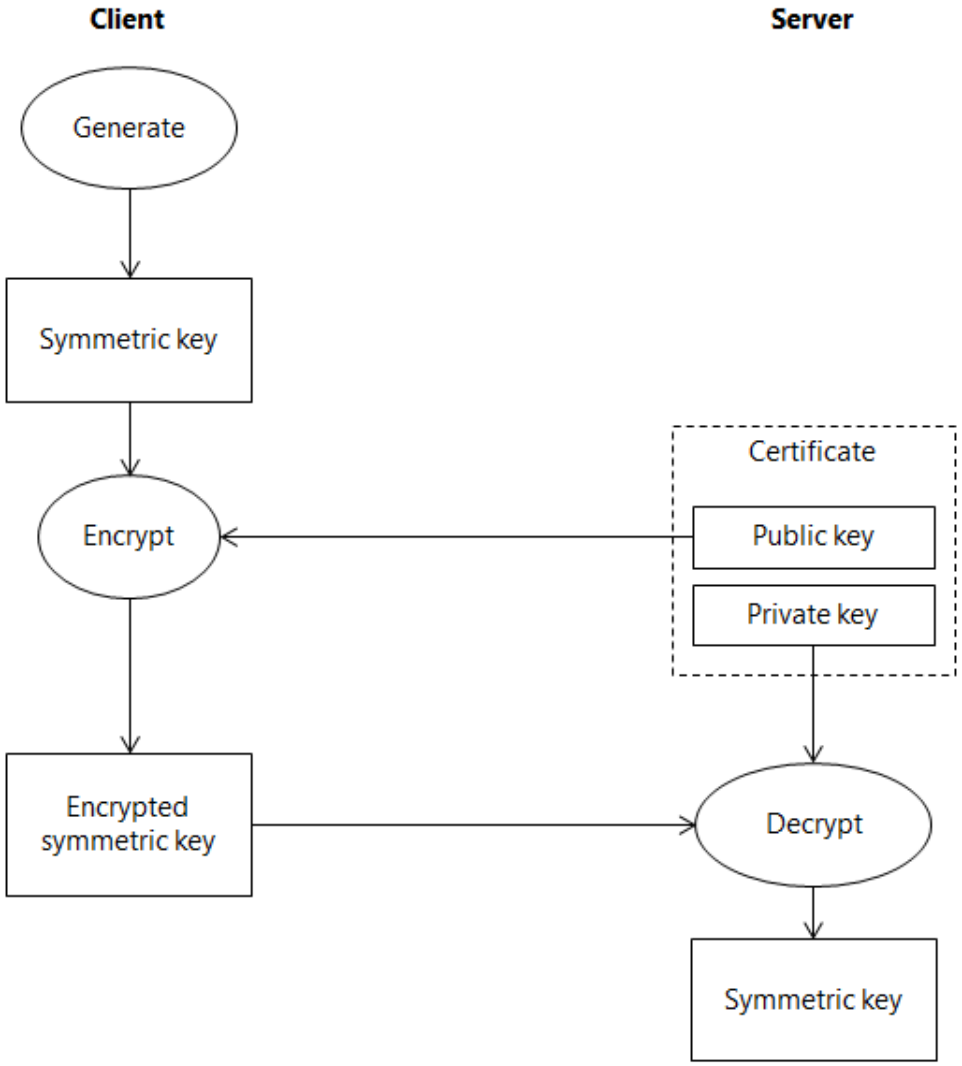


A tanúsítvány ellenőrzése

4. Nem vonták vissza.

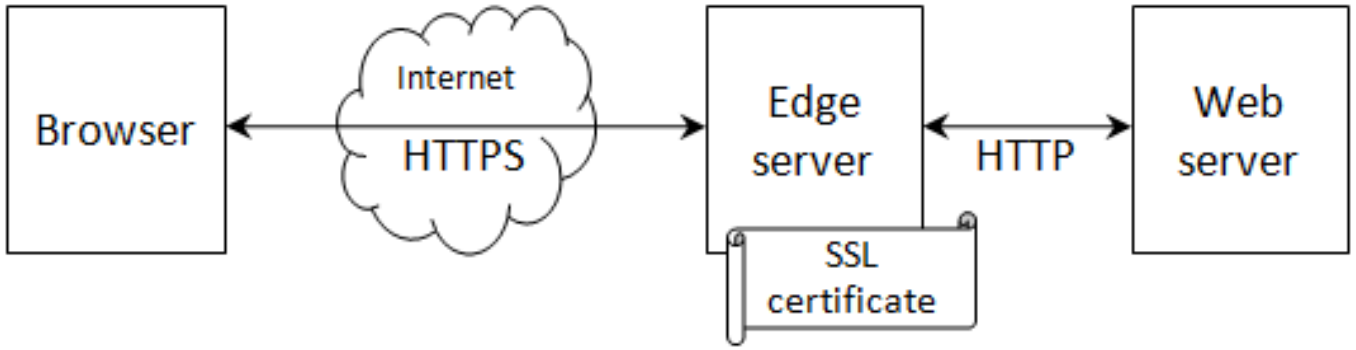
- A tanúsítvány vagy a CA kompromittálódhat.
  - 2001: VeriSign „Microsoft Corporation”
  - 2011. március: iráni hekkerek Comodo tanúsítványokkal man-in-the-middle támadásokat hajtottak végre.
  - 2012: Trustwave adott ki subordinate root CA tanúsítványt, amit később MITM támadásokkal lehallgatáshoz használtak.
- Certificate Revocation List
  - Aláírt, TTL-lel (24 óra) ellátott, nyilvános lista.
  - A tanúsítványban lévő CRL Distribution Point határozza meg az URL-t.
- Online Certificate Status Protocol (OCSP, RFC 6960)
  - Egy tanúsítvány státuszának lekérdezésére a CA-tól.
  - A kliensnek nem kell a teljes CRL-t feldolgoznia.

A kulcscsere folyamata



SSL termination

- Tévhit: az SSL túlságosan terheli a szervert.
- 2010. január: Gmail HTTPS átállás
  - > +1% CPU, +10kB memory/connection, +2% network overhead
- A webszerver tehermentesítése (offloading) a HTTPS forgalommal járó kriptográfiai feladatoktól.
- Szerver farm esetén is jó, mert nem kell minden webszerverre telepíteni a tanúsítványt.



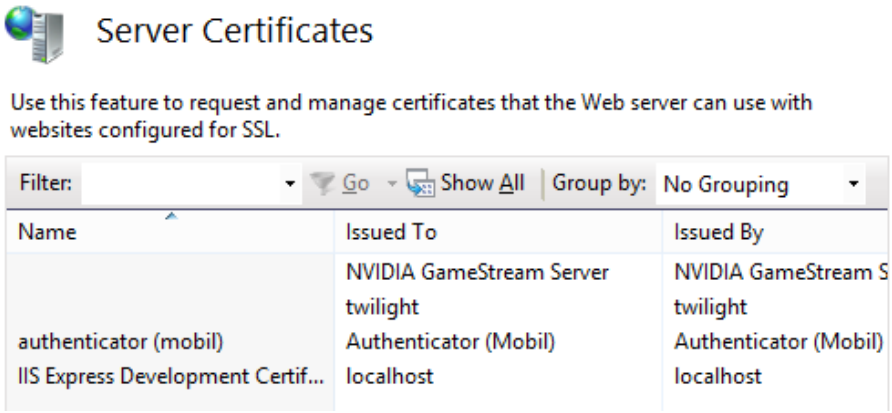
https://www.imperialviolet.org/2010/06/25/overclocking-ssl.html

Gyakorlati megfontolások I.

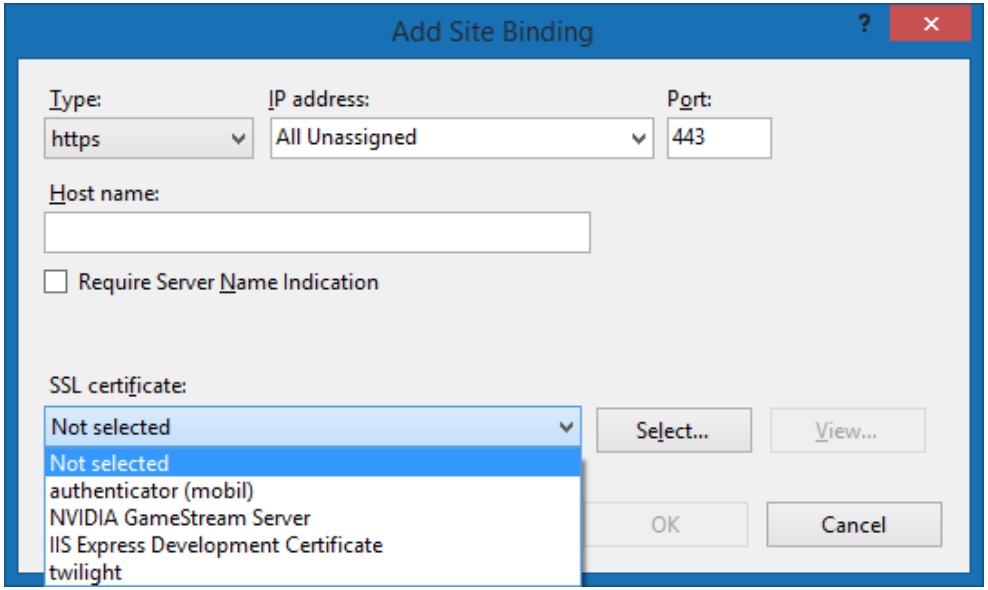
- Rövid ellenőrző lista:
  - Minden érzékeny adat HTTPS-en megy.
  - HTTPS oldalakra nem kerül HTTP tartalom.
  - Authentikációs sütik
    - nem mennek HTTP-n.
    - a Secure flag be van állítva.
  - A bejelentkező oldalak is HTTPS-en mennek.

IIS beállítás

- IIS Manager
  - > Server Certificates



- Site binding



Gyakorlati megfontolások II.

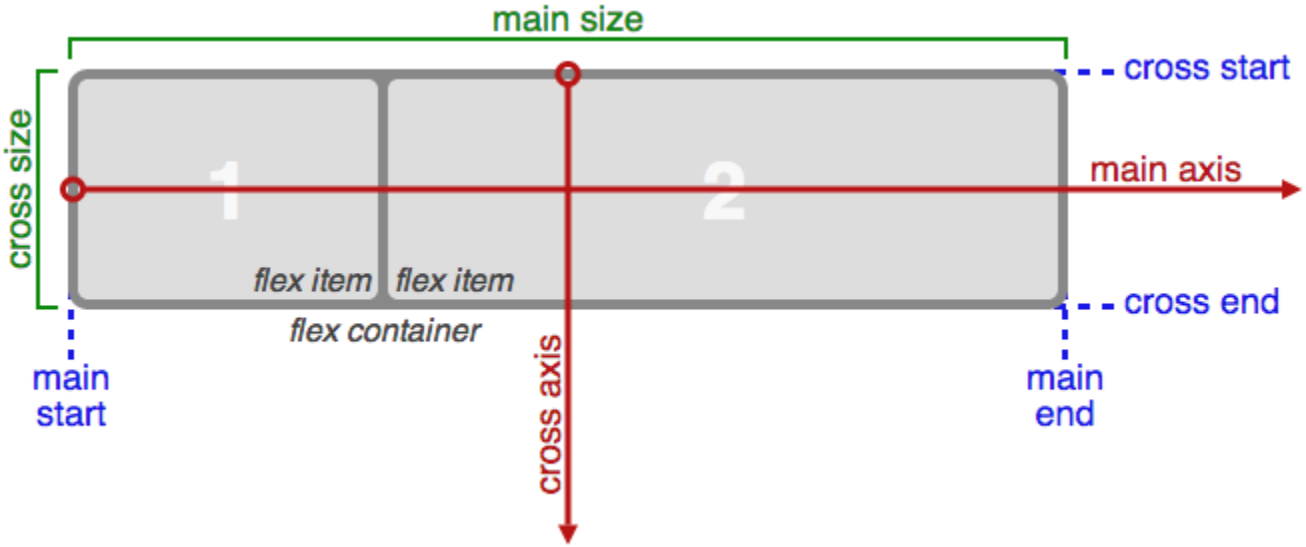
- A teljes HTTPS forgalom néha nem megvalósítható
  - A mixed contentet el kell kerülni, ehhez a felhasznált szolgáltatásoknak támogatnia kell a HTTPS-t:
    - Ad network
    - Image hosting service
    - Külső szolgáltatókból beágyazott tartalom
      - Gravatar, Facebook, Google Analytics
  - A CDN drágább lesz.
  - A terheléselosztóknak támogatniuk kell az SSL offloadingot.
  - Több domain esetén több tanúsítvány és azok folyamatos karbantartása.
  - Ha volt már korábban HTTP, akkor az átállásnak SEO következményei lehetnek.

Flexbox

Modern Layout készítése

Mit old meg a flexbox?

- Teljes(ebb) kontrollt ad egy konténer gyerekei felett, reszponzív módon
  - Elemek igazítása egymáshoz és a konténer széleihez képest
  - Elemek automatikus méretezése arányosan
  - Elemek sorrendjének variálása



Flexbox tulajdonságok (konténer)

- `display:flex` a konténeren, a bekapcsoláshoz
- `flex-direction`: gyerekek elrendezése
  - vízszintes (`row`) vagy
  - függőleges (`column`) tengely mentén.
- `flex-wrap`: Sor-/oszloptörés engedélyezése.
- `justify-content`: elemek rendezése, tagolása a főtengely mentén

justify-content

Flexbox: justify-content és flex-grow

A PEN BY Gincsai Gábor

Save | Fork | Settings | Change View

HTML

```
<div id="main">
  <div style="background-color:coral;"></div>
  <div style="background-color:lightblue;"></div>
  <div style="background-color:khaki;"></div>
  <!-- Ő kapjon flex-grow: 1-et -->
  <div style="background-color:pink;" class="grow">
</div>
</div>
```

CSS

```
#main {
    width: 400px;
    height: 70px;
    border: 1px solid #c3c3c3;
    display: flex;
    justify-content: space-between;
    /*justify-content: space-around;*/
    /*justify-content: space-evenly;*/
}
#main div {
    width: 60px;
    height: 60px;
}
/*.grow{
  flex-grow: 1;
}*/
```

https://codepen.io/gincsai/pen/POPMBg

A flex-start és a flex-end értelmezése

	flex-start	flex-end
row	balra	jobbra
row-reverse	jobbra	balra
column	fentre	lentre
column-reverse	lentre	Fentre

További konténer tulajdonságok

- `align-items`: a gyerekek igazítása a főtengelyre merőlegesen.
  - Hasonlít a `justify-content`-re, de fontos különbség, hogy nem a *gyerekek között megmaradt* helyet osztja be, hanem a gyerekek és a *flexbox széle* közötti helyet.
  - Tehát ez akkor is működik, ha valamelyik gyerek „nyúlós” (mivel az a főtengely mentén nyúlik).
  - A gyerekek a kereszttengelyen is nyújthatók, erre van a `stretch` opció
    - Gyakori hiba azt hinni, hogy a `justify-content` rendelkezik `stretch` értékkel, de nincs neki, mivel a főtengelyi menti nyúlást a „gyerekek döntik el” (`flex-grow`, ld. később)

align-items

HTML

```
<div id="main">
  <div style="background-color:coral;">
    Első rövid oszlop.
  </div>
  <div style="background-color:lightblue;">
    Második kicsivel hosszabb szövegű oszlop.
  </div>
  <div style="background-color:khaki;">
    Harmadik
  </div>
  <!-- Ő kapjon flex-grow: 1-et -->
  <div style="background-color:pink;">
    Negyedik oszlop, aminek a szövege nagyon-nagyon nagy.
  </div>
</div>
```

CSS

```
#main {
    width: 400px;
    height: 150px;
    border: 1px solid #c3c3c3;
    display: flex;
    align-items: flex-start;
    /*align-items: center;*/
    /*align-items: flex-end;*/
    /*align-items: baseline;*/
    /*align-items: stretch;*/
}
#main div {
    width: 70px;
    min-height: 60px;
}
```

https://codepen.io/gincsai/pen/YEwKaK

További konténer tulajdonságok

- `align-content`: többsoros flexbox *sorainak* igazítása a kereszttengely mentén.
  - Egysoros flexboxra nincs hatása.
  - Értékei kb. ugyanazok és kb. ugyanazt jelentik, mint a `justify-content` esetén, azonban itt van külön `stretch` érték is (ami a default), hiszen itt nem a főtengelyről, hanem a kereszttengelyről van szó, tehát nem a gyerekektől függ a „nyúlás”.

Flexbox gyerek tulajdonságai

- `flex-grow`: szabályozza, hogy a gyerek nyúljon-e – és a többiekhez képest milyen arányban –, ha marad hely a főtengely mentén. Alapértelmezett: 0 (nincs nyúlás)
- `flex-shrink`: összenyomható-e a gyerek, ha kevés a hely, és nem lehet sort törni; és ha igen, milyen arányban.
  - Alapértelmezett: 1
- `flex-basis`: a gyerek alap mérete nyújtás/összenyomás előtt, alapértelmezetten `auto`.
- `flex`: shorthand az előző háromra.
  - `flex: 1 1 auto` – teljesen „rugalmas”
  - `flex: 0 0 auto` – teljesen „rugalmatlan”

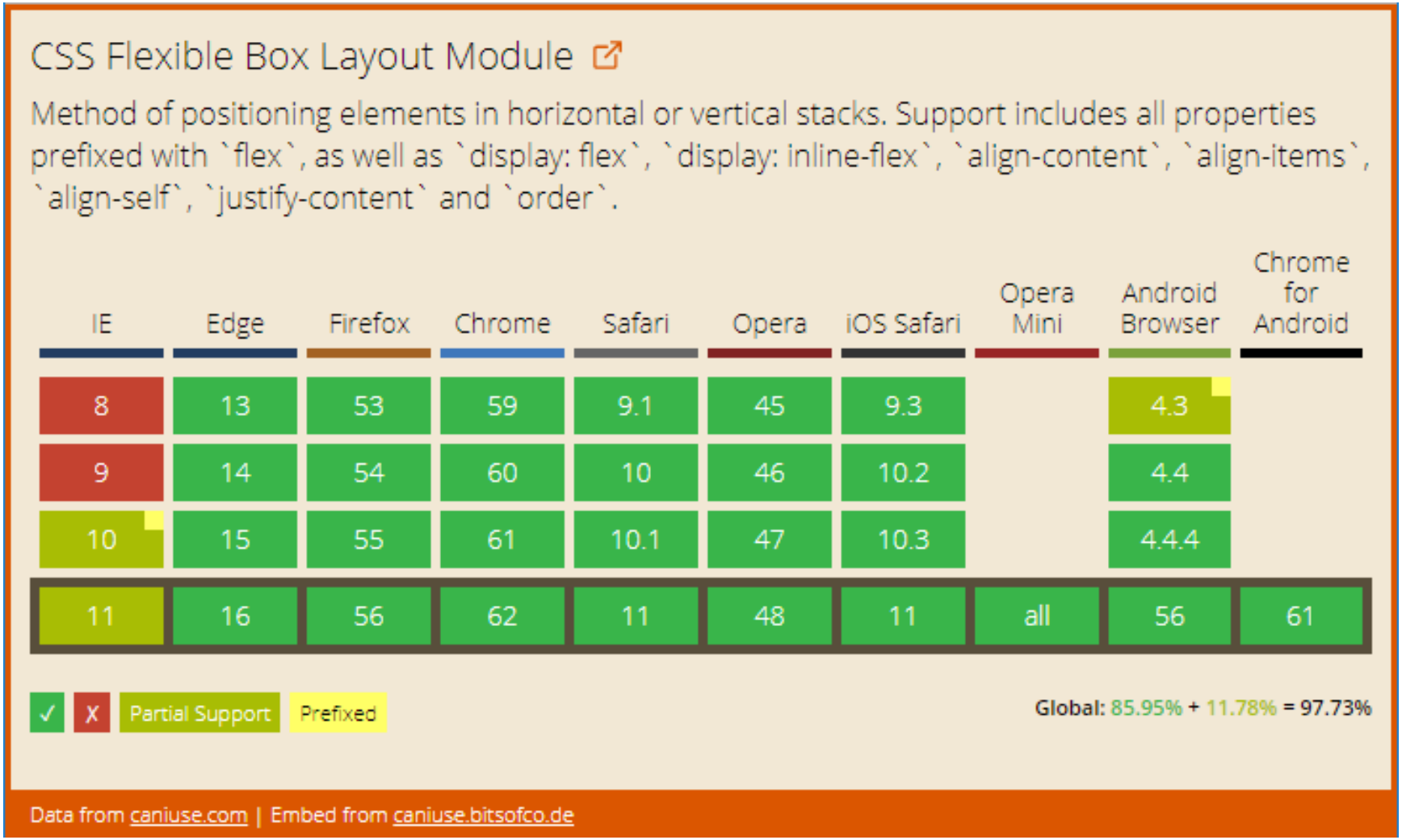
flex-basis részletek

- Alapértelmezett értéke az `auto`, ami a gyerek főtengely menti méretét (`width` vagy `height`) értékét veszi fel.
  - Ha az *is* `auto`, akkor a tartalomhoz igazodik a méret.
- Megadhatunk konkrét értéket is (pl. 25px, 33%), ezzel effektíve felülírjuk a főtengely menti méretet.
  - Ez akkor lehet hasznos, ha variáljuk a tengelyt (pl. mobil nézet), és emiatt simán a `width` vagy a `height` felülírása nem lenne elég rugalmas.

További flexbox gyerek tulajdonságok

- `align-self`: a gyerek „felülírhatja” saját magára a konténeren beállított `align-items` értéket.
- `order`: a gyerekek alapvetően abban a sorrendben jelennek meg, ahogy az a HTML-ben szerepel. Az `order`-rel ezen variálhatunk.
  - Negatív szám is lehet, alapértelmezetten 0.
- Van néhány „hagyományos” CSS tulajdonság, ami nem alkalmazható flexbox gyerekekre.
  - `float`, `clear`, `vertical-align`

Használhatom a flexboxot?



CSS Flexible Box Layout Module

Method of positioning elements in horizontal or vertical stacks. Support includes all properties prefixed with `flex`, as well as `display: flex`, `display: inline-flex`, `align-content`, `align-items`, `align-self`, `justify-content` and `order`.

IE	Edge	Firefox	Chrome	Safari	Opera	iOS Safari	Opera Mini	Android Browser	Chrome for Android
8	13	53	59	9.1	45	9.3		4.3	
9	14	54	60	10	46	10.2		4.4	
10	15	55	61	10.1	47	10.3		4.4.4	
11	16	56	62	11	48	11	all	56	61

✓ X Partial Support Prefixed

Global: 85.95% + 11.78% = 97.73%

Data from caniuse.com | Embed from caniuse.bitsofco.de

DEMO

Flexbox használata

https://codepen.io/gincsai/pen/eeJYmb

align-items, justify-content, flex-wrap, flex-shrink, flex-grow

BME AUT
Automatizálási és
Alkalmazott
Informatikai Tanszék