Számítógépes biztonsági kultúra

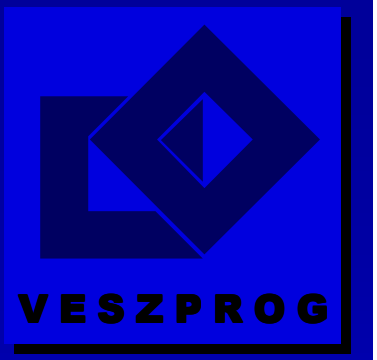
Dr. Leitold Ferenc
Veszprémi Egyetem - Veszprog Kft.
fleitold@veszprog.hu

Az elektronikus aláírás használatának biztonsági problémái

VESZPROG Kft.

Dr. Leitold Ferenc
fleitold@veszprog.hu

Példa

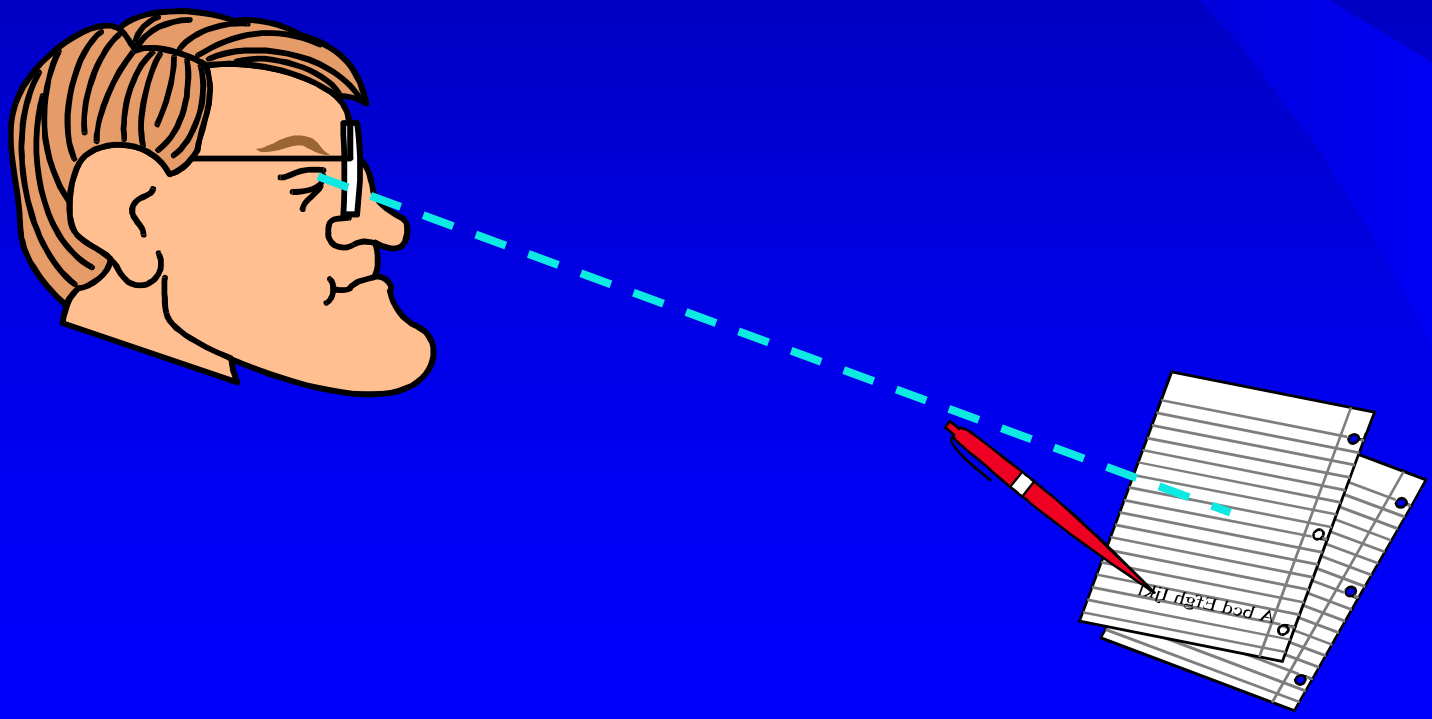


Jelenthet-e a digitális aláírás a hagyományos aláíráshoz képest további veszélyeket ?

➔ **IGEN**

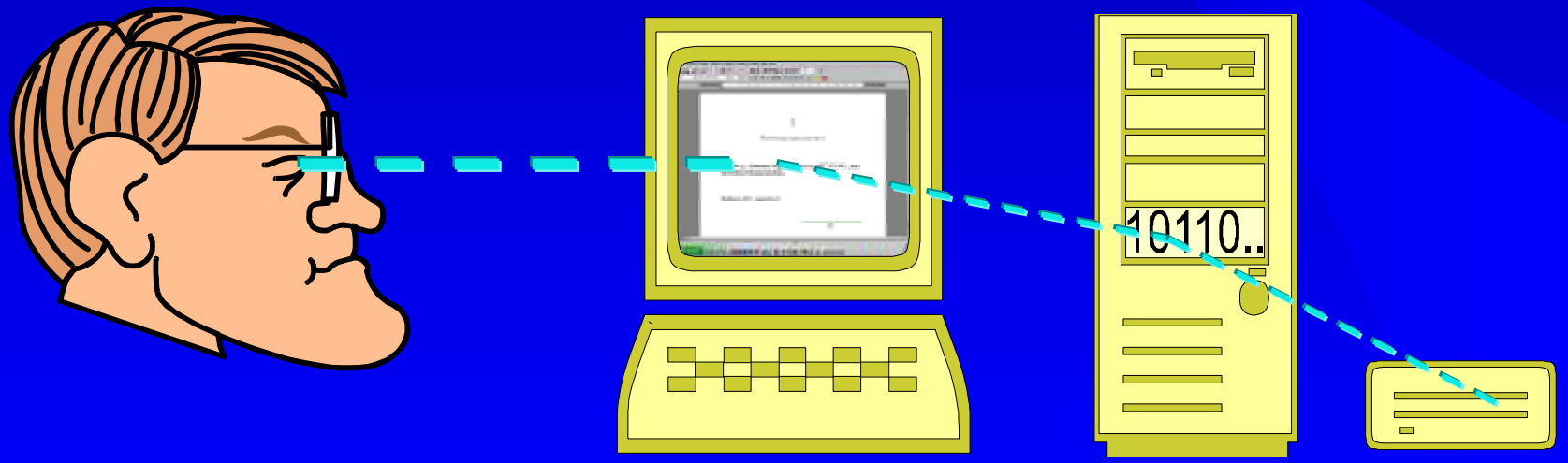
Hagyományos aláírás

VESZPROG



Elektronikus aláírás

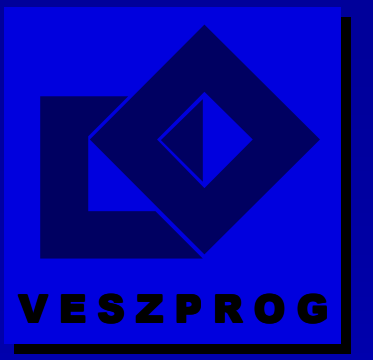
VESZPROG



Támadási lehetőségek

- Megjelenítés befolyásolása
- Aláírási folyamat manipulálása

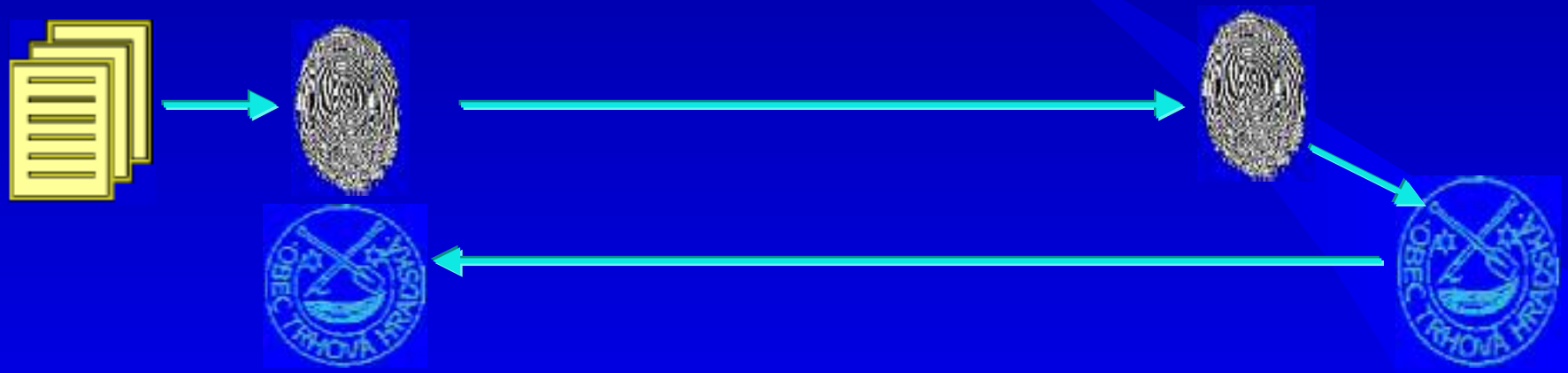
Megjelenítés befolyásolása



- Betűtípus módosítása
  - Windows, X: font file-ok
  - VGA: font-ok letöltési lehetősége
- Dokumentumhoz kapcsolt, automatikus program (makró)
- Megjelenítő program módosítása
- ...

Aláírási folyamat manipulálása

VESZPROG



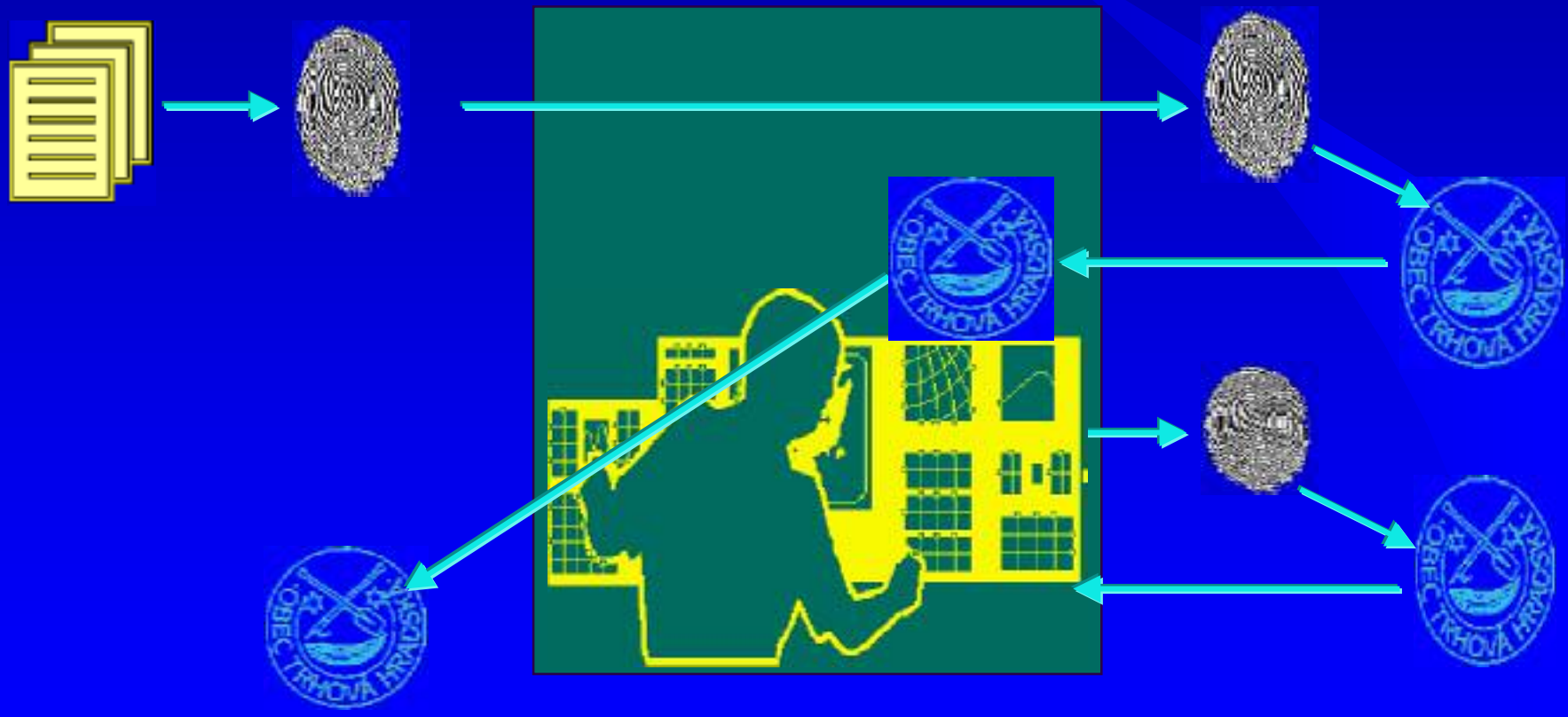
Felhasználói felület

Windows + soros vonal

Aláíró eszköz

Aláírási folyamat manipulálása

VESZPROG

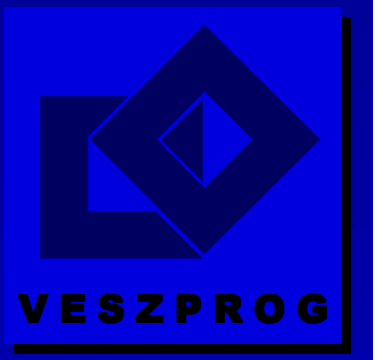


Felhasználói felület

Windows + soros vonal

Aláíró eszköz

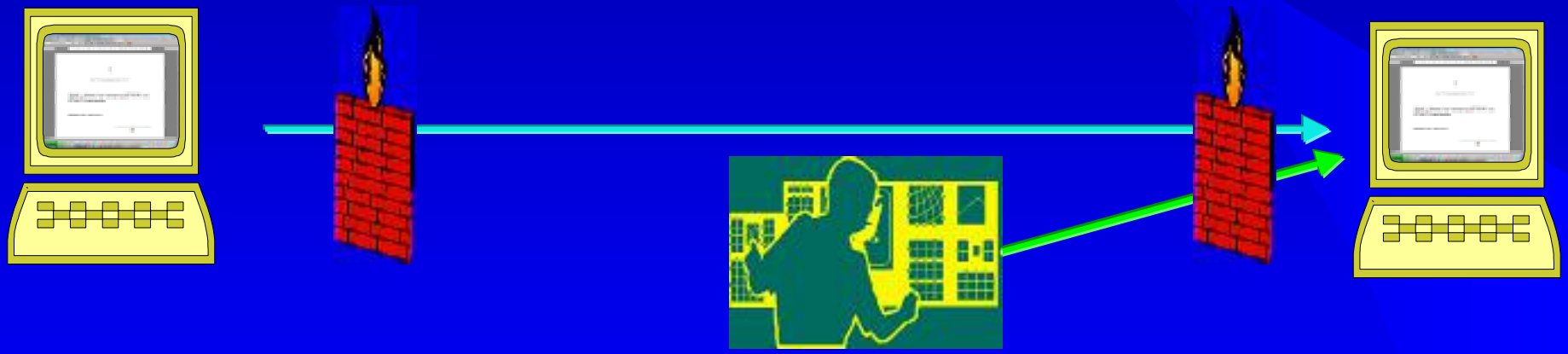
Aláírási folyamat manipulálása



- Felhasználói felület és az aláíró eszköz közti kommunikáció felügyelése
- Aláíró program módosítása
- ...

Elektronikus aláírás továbbítása

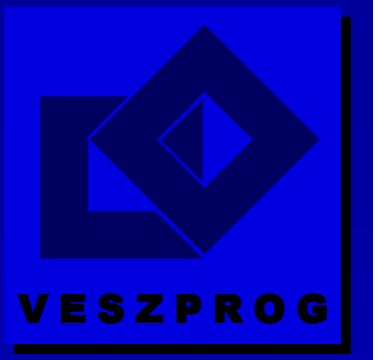
VESZPROG



Titkosítva vagy titkosítás nélkül ?

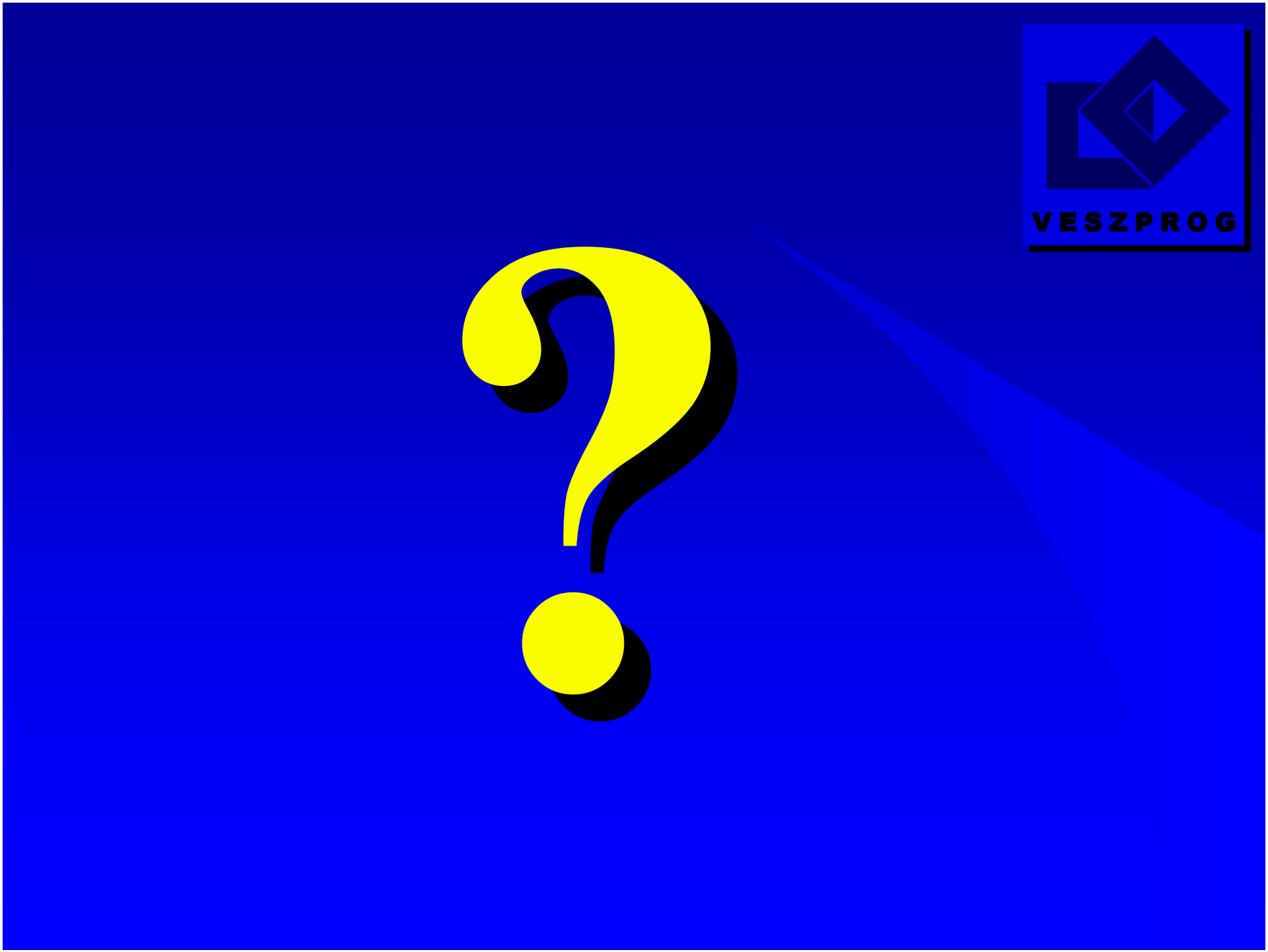
A tűzfal átengedi a titkosított üzenetet ?

Összegzés



Nem mindegy, hogy

- **mit írunk alá,**
- **milyen aláíró eszközt használunk,**
- **milyen célból szeretnénk digitálisan aláírni.**


VESZPROG