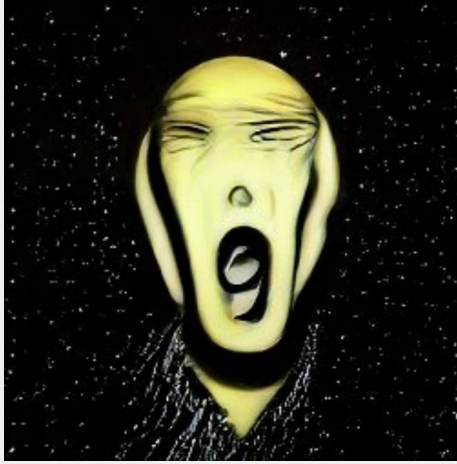


# Screaming into the void: All e-signatures in the world are broken!

@KirilsSolovjovs on twitter

https://kirils.org for more

Mg.sc.comp.,Mg.phys. Kirils Solovjovs

Possible Security, EDI

# Who?

Kirils Solovjovs

- Institute of Electronics and Computer Science
- Possible Security
- Hack Hack Hack!
- kirils.org

# Other research

- 2017 How they SHAttered Latvian eID
- 2020- 2023 WearSec

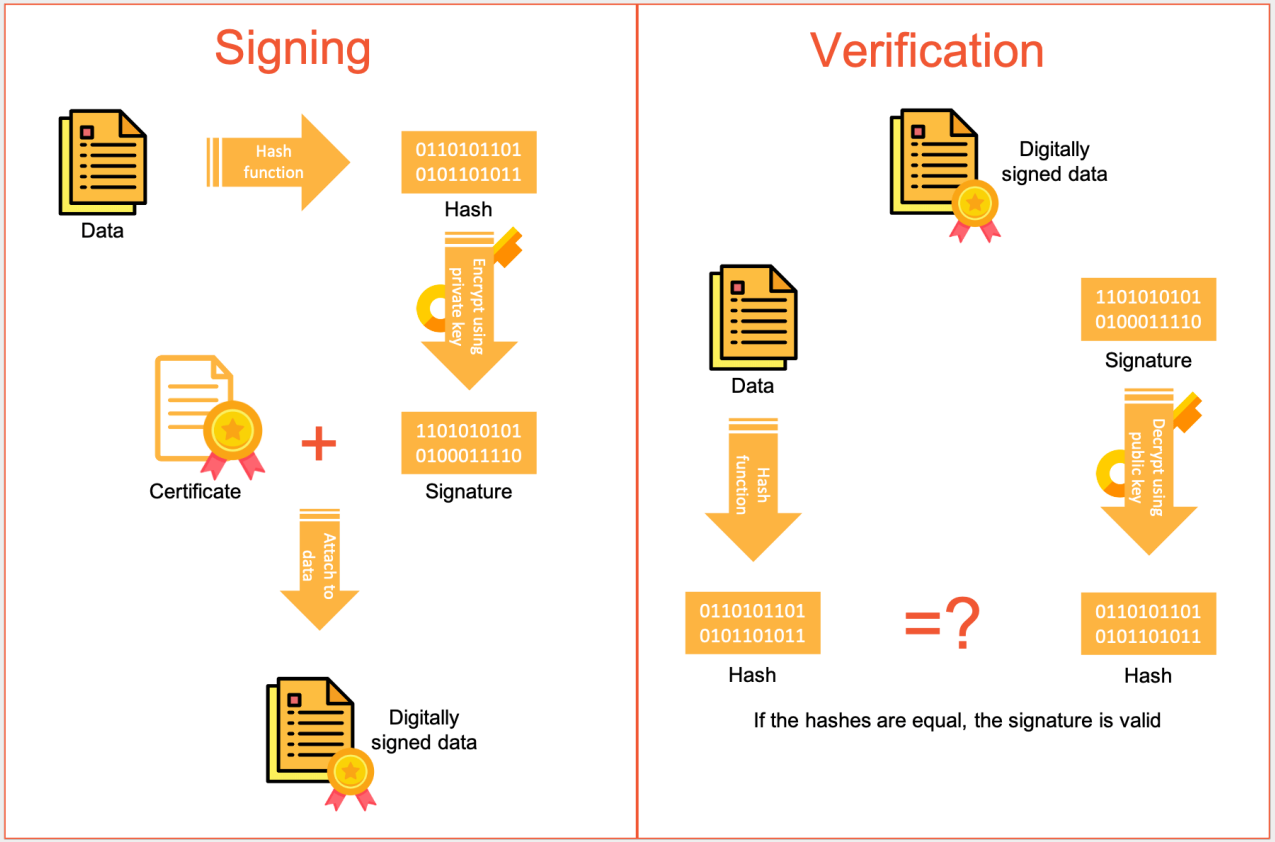

Latvian Council of Science project no. LZP-2020/1-0395 “Automated wireless security analysis for wearable devices” (WearSec) – device identification and vulnerability analysis (fingerprinting & fuzzing)

# What?

- Who is this for?

- How digital signatures work
- How we perceive content
- Attacks
- Disclosure
- What's next

# Signatures



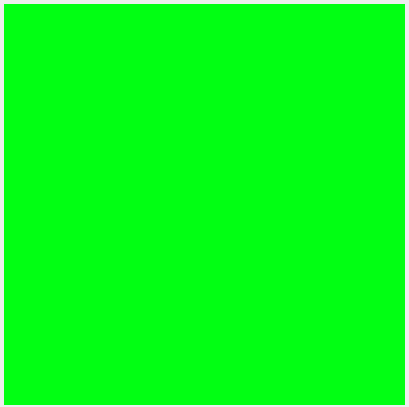

frevvo.com

# EU Signatures

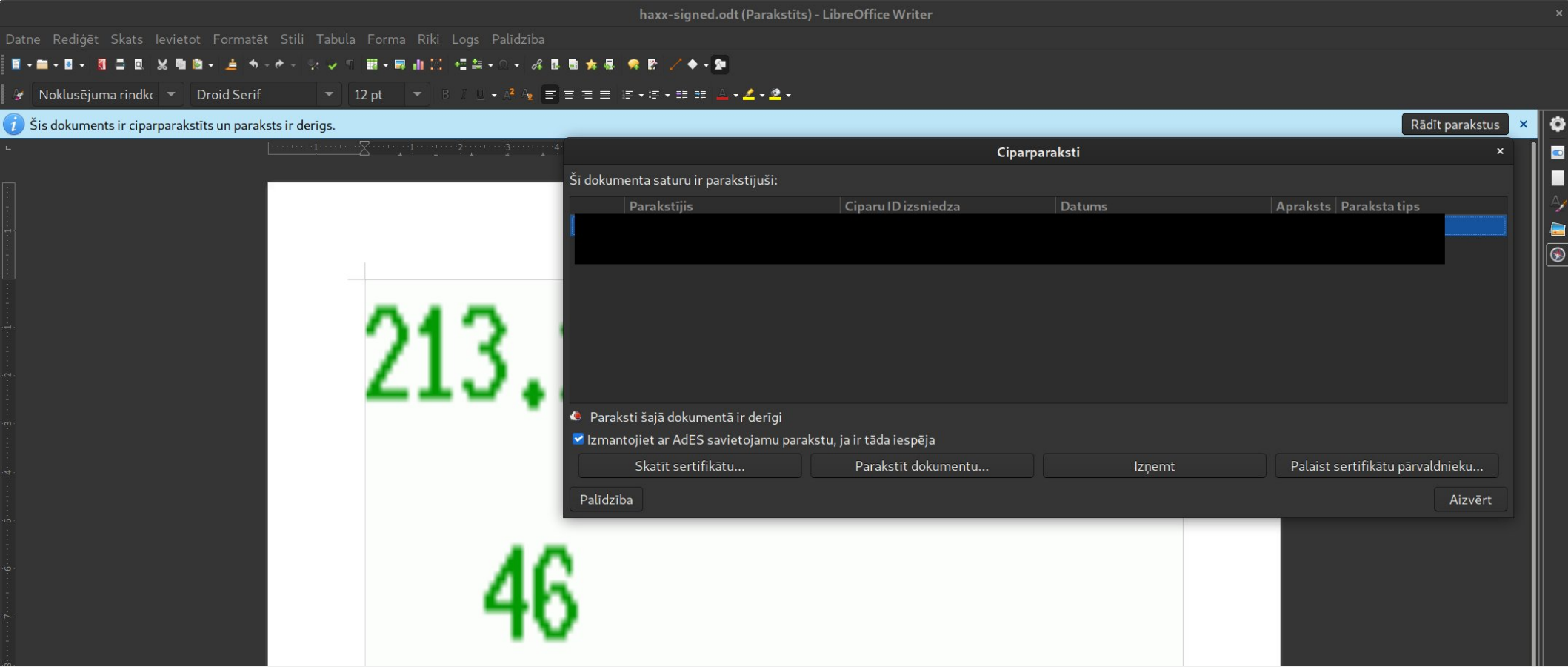
- PDF
- ASICE ← container!
- eDoc ← container!
- …

# Dynamic content

- Dynamic OLE objects
- Static object pre-renders
- Remote content
- (for classic document formats)
- but it fully depends on the format. ELF? :)



# DEMO


haxx-signed.odt (Parakstīts) - LibreOffice Writer
Datne Rediģēt Skats Ievietot Formatēt Stili Tabula Forma Rīki Logs Palīdzība
Noklusējuma rindk
Droid Serif
12 pt
Šis dokuments ir ciparparakstīts un paraksts ir derīgs.
Rādīt parakstus
Ciparparaksti
Šī dokumenta saturu ir parakstījuši:
Parakstījis
Ciparu ID izsniedza
Datums
Apraksts
Paraksta tips
Paraksti šajā dokumentā ir derīgi
Izmantojiet ar AdES savietojamu parakstu, ja ir tāda iespēja
Skatīt sertifikātu...
Parakstīt dokumentu...
Izņemt
Palaist sertifikātu pārvaldnieku...
Palīdzība
Aizvērt
213.
46

# Does it **really** matter?

- Apparent tampers
- Fraud prosecution

# WONTFIX

- See previous slide :)
- But what if we could make a document that appears a 100% legit?

# Remote content!

- :-(

# Can we even fix it?

- It can't be solved technologically
- It can't be solved politically

# What are we gonna do about it then?

# Q&A

Slides are available on https://kirils.org

Find me on twitter: @KirilsSolovjovs