

Seminar 2021

MA Program , CS&C

Approach, Seminar formula

login: student

password: mgrj23



topic

3-4 or more presentations

per team



final report - recommendation

technical &....

(business summary 1
page 30)



presentations:

slides, present of product

blackboard

explain

core issues.

speaking skills.

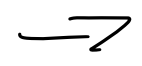
research level

knowledge transfer

teamwork

propose topics:

person



team



schedule

new topic

Topic - 1 e-voting

- 1) o mail-in / instant
- 2) o small groups / large scale
- 3) o verifiability
- 4) o devices

ad 1) Apollo, Helios

ad 2) scale

ad 3) key issue!

ad 4) malicious

ad 5) future

before:

gov. ↔ Estonia

Norway *

USA

CH



exam PhD, habilitation

remote

formal

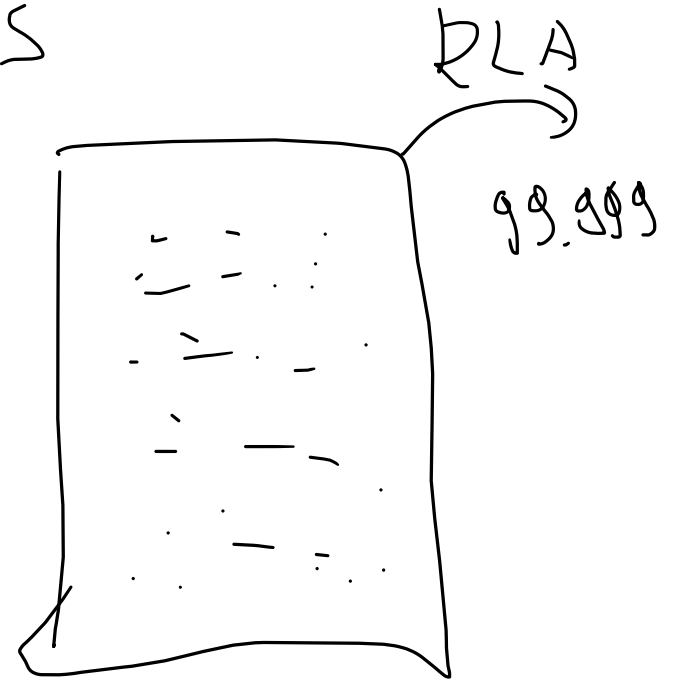
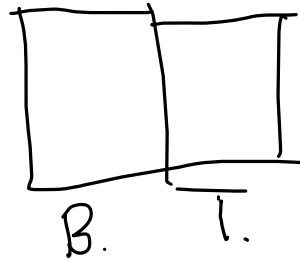
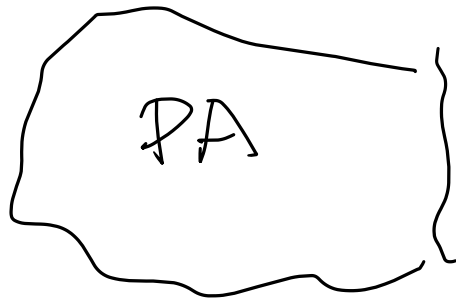
many examiners

protocol

tech reality

dr Zagórski - Remote equity

- risk limiting audits



⇒ RLA compulsory in some state

practice:

web for-ular

→ clicking

server returns the results

no proof of correctness



Recommendation for:
medium

a) small enterprises

b) public bodies

c) education

how chaos!

Topic - 2 securing digital documents

- o signatures / digital stamps
- o distributed ledger
- o **B&B**
- o "David & Goliath"

now:

scans for administration
effort doubled
master copy

David:

user, company

Goliath: (NSA, -Crime, ...)

very powerful:

research
machines
trapdoors

Scheme

Secure even with Goliath

- information theoretic security

- "subversion resistance"

Recommendation

what to do now!

Topic 3 -GDPR

- o cookbook / methodology
- o solution proposals for hard problems
- o protection technologies

SME

lowers:



'Safe Harbour'
2000 EC

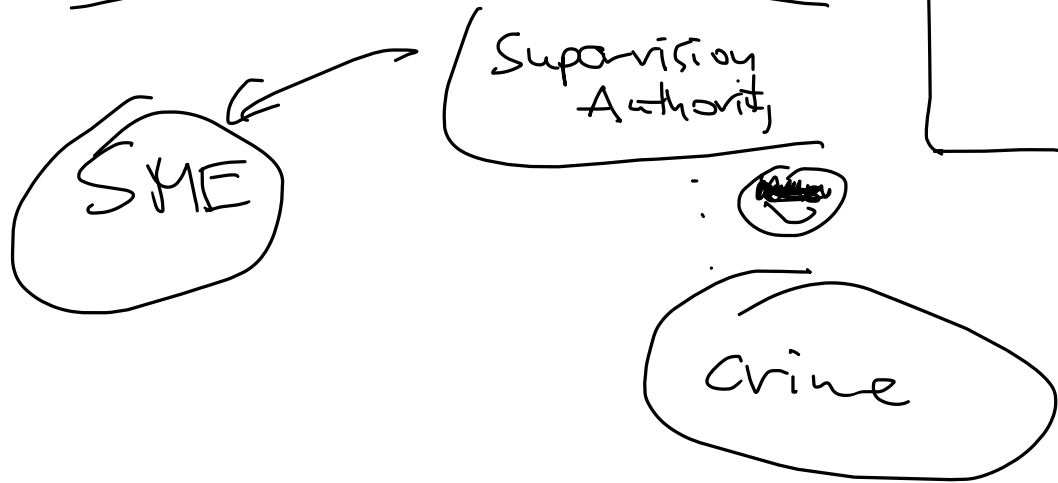
'Privacy Shield'
2016

2020, July
TSUE
P.Sh. is nothing
'46, not 45

M. Yung (Google)
myself
dr Lukas-Dutka

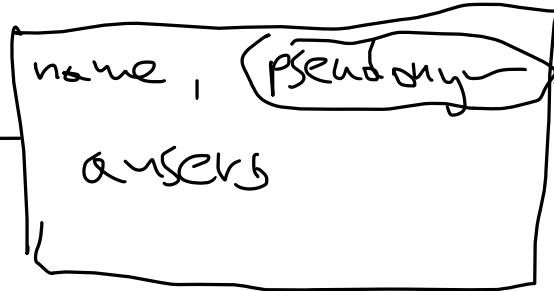
plenty problems
one cannot implement
GDPR as it is

EU Report 2020
≈ "it's fine"



good practices:
- exam:

Self Serv... ID



ps.	5.0
ps	4.5

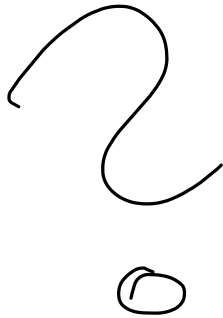
Topic - 4 subversion resilience

- o everybody is cheating!
- o protection on application level

What to do?

Topic 5 Cyptocurriencies & co

now
future?



Bitcoin:

202x, EC - Bitcoin forbidden
burning coal, gas, - -

Argentina power consumpt. \approx Bitcoin

Topic 6

continuous

authentication