AFTER THE SERVER SIGNING..

Katrin Laas-Mikko, Kalev Pihl

EIDAS FOCUS

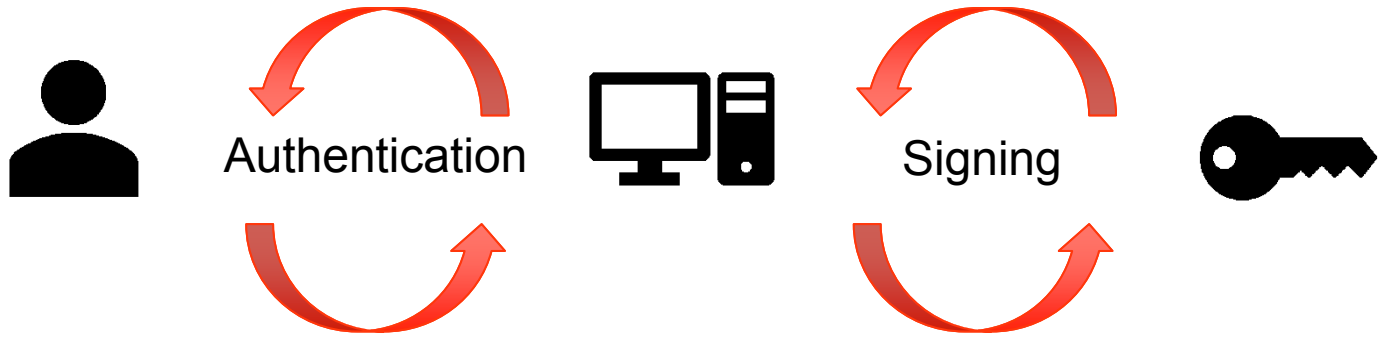
SK ID SOLUTIONS

+ PKI obsession
+ Environment not considered

LEAP

SK ID SOLUTIONS

- You know who I am – therefore you can sign stuff in my name as many times as you wish!



NOT A TRUST SERVICE

TRUST SERVICE

STATE OF ART SSS

ID SOLUTIONS

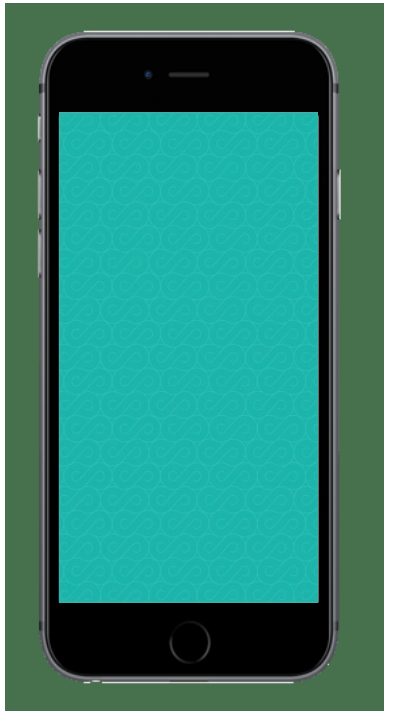
- From the TOE:
- *It is possible to define a certain time period where after the two factor authentication it will be possible to sign several digital signature operations within the same application*

- From eIDAS:
- *It is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control*

BETTER SERVER SIGNING

ID SOLUTIONS

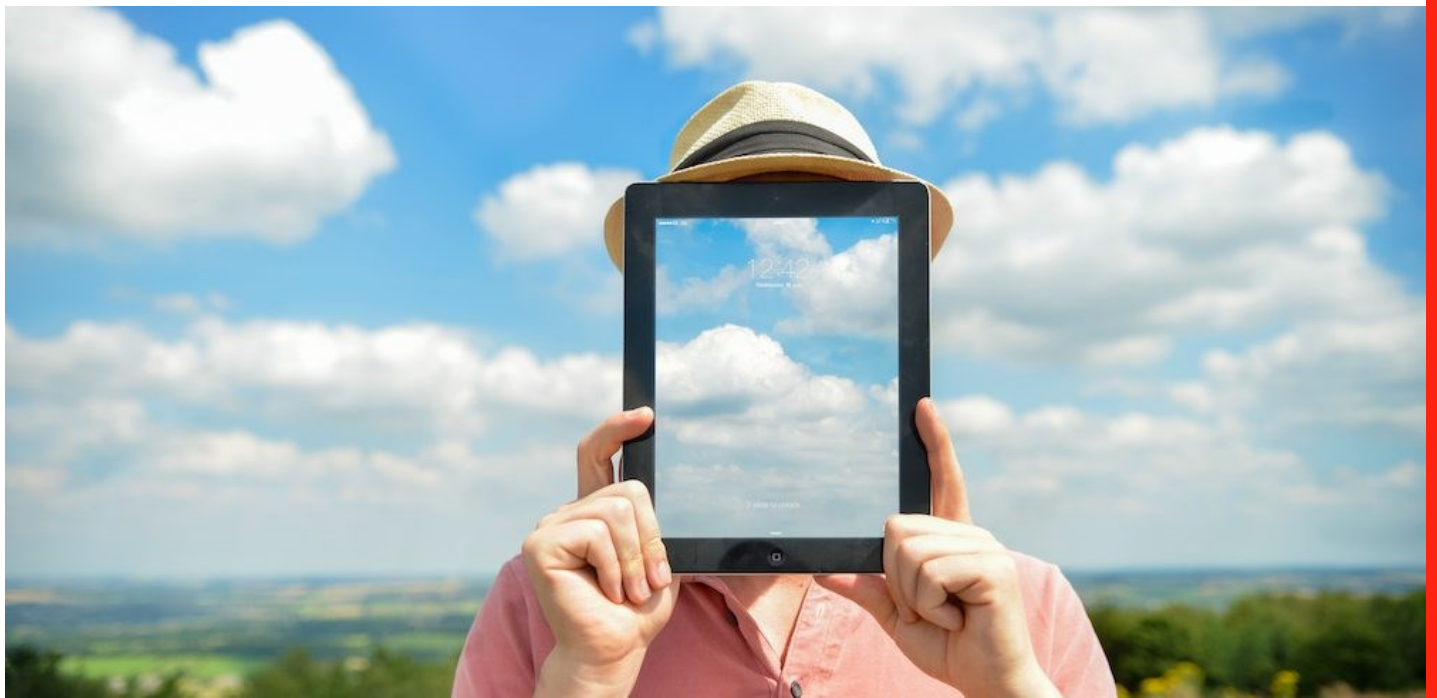
- You cannot sign anything under my name without my involvement
- Still not considering the environment enough



GOOD (SERVER) SIGNING

ID SOLUTIONS

+ Signature transparency!



QSEAL

ID SOLUTIONS

- Server implementations, massive amounts of data sealed in the name of the company.
  - Leave the CEO signature only to the places where she really has time to think it through!
- NOT SO!

POSSIBILITIES

THAT WE KNOW OF

ID SOLUTIONS

- QSCD personalised in TSP premises and released then to the owners
- QSCD SSS in the premises of TSP

- NQ Seal

QSEALCD

ID SOLUTIONS

- From the TOE
  - *Remark:*

  *In the following paragraphs, it will be presented that ***** can be installed as a Seal Creation Device.*

  In this case only one factor, which is based on a static password, is required for producing a digital signature.

SK ID SOLUTIONS

GO DO …

… maintain the eIDAS meaning – do not just implement the technical fixes!

THANK YOU!

SK ID SOLUTIONS