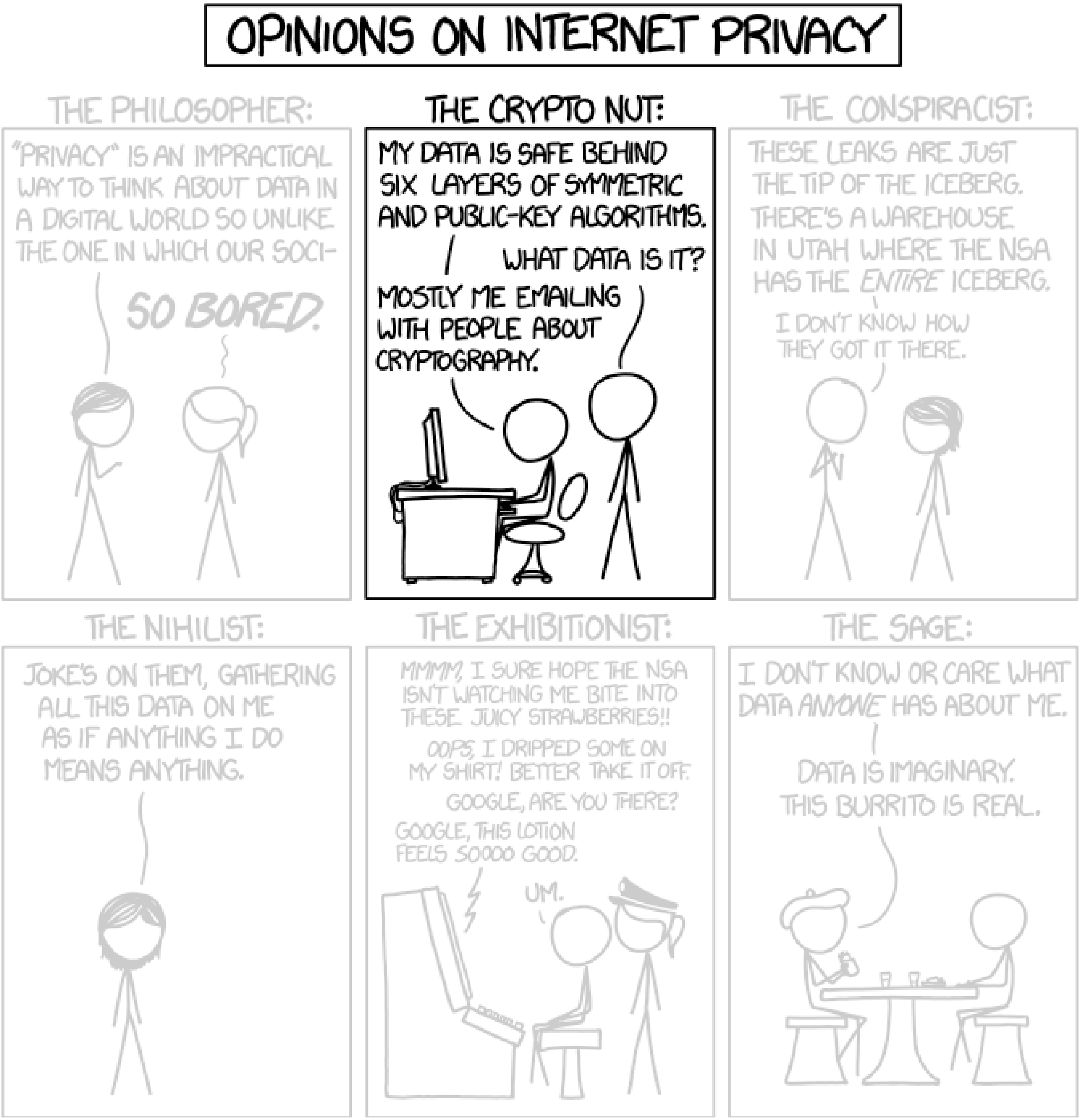
Security Technologies

Privacy Enhancing Technologies

KARLSTAD
UNIVERSITY
SWEDEN

Leonardo A. Martucci

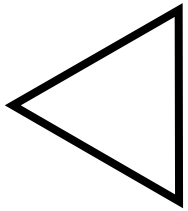

OPINIONS ON INTERNET PRIVACY
THE PHILOSOPHER:
"PRIVACY" IS AN IMPRACTICAL WAY TO THINK ABOUT DATA IN A DIGITAL WORLD SO UNLIKE THE ONE IN WHICH OUR SOCI-
SO BORED.
THE CRYPTO NUT:
MY DATA IS SAFE BEHIND SIX LAYERS OF SYMMETRIC AND PUBLIC-KEY ALGORITHMS.
WHAT DATA IS IT?
MOSTLY ME EMAILING WITH PEOPLE ABOUT CRYPTOGRAPHY.
THE CONSPIRACIST:
THESE LEAKS ARE JUST THE TIP OF THE ICEBERG. THERE'S A WAREHOUSE IN UTAH WHERE THE NSA HAS THE ENTIRE ICEBERG.
I DON'T KNOW HOW THEY GOT IT THERE.
THE NIHILIST:
JOKE'S ON THEM, GATHERING ALL THIS DATA ON ME AS IF ANYTHING I DO MEANS ANYTHING.
THE EXHIBITIONIST:
MMMM, I SURE HOPE THE NSA ISN'T WATCHING ME BITE INTO THESE JUICY STRAWBERRIES!!
OOPS, I DRIPPED SOME ON MY SHIRT! BETTER TAKE IT OFF.
GOOGLE, ARE YOU THERE?
GOOGLE, THIS LOTION FEELS SOOOO GOOD.
UM.
THE SAGE:
I DON'T KNOW OR CARE WHAT DATA ANYONE HAS ABOUT ME.
DATA IS IMAGINARY. THIS BURRITO IS REAL.

https://www.xkcd.com/1269/

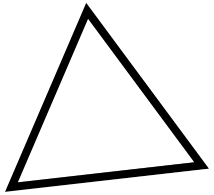
Security Technologies

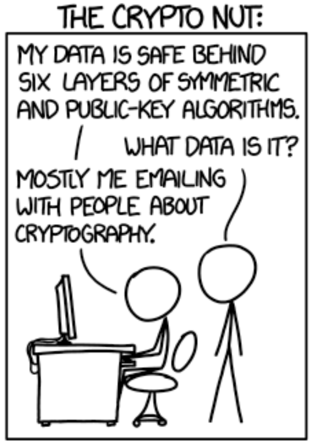
Have Objectives:

- Confidentiality
- Integrity
- Availability



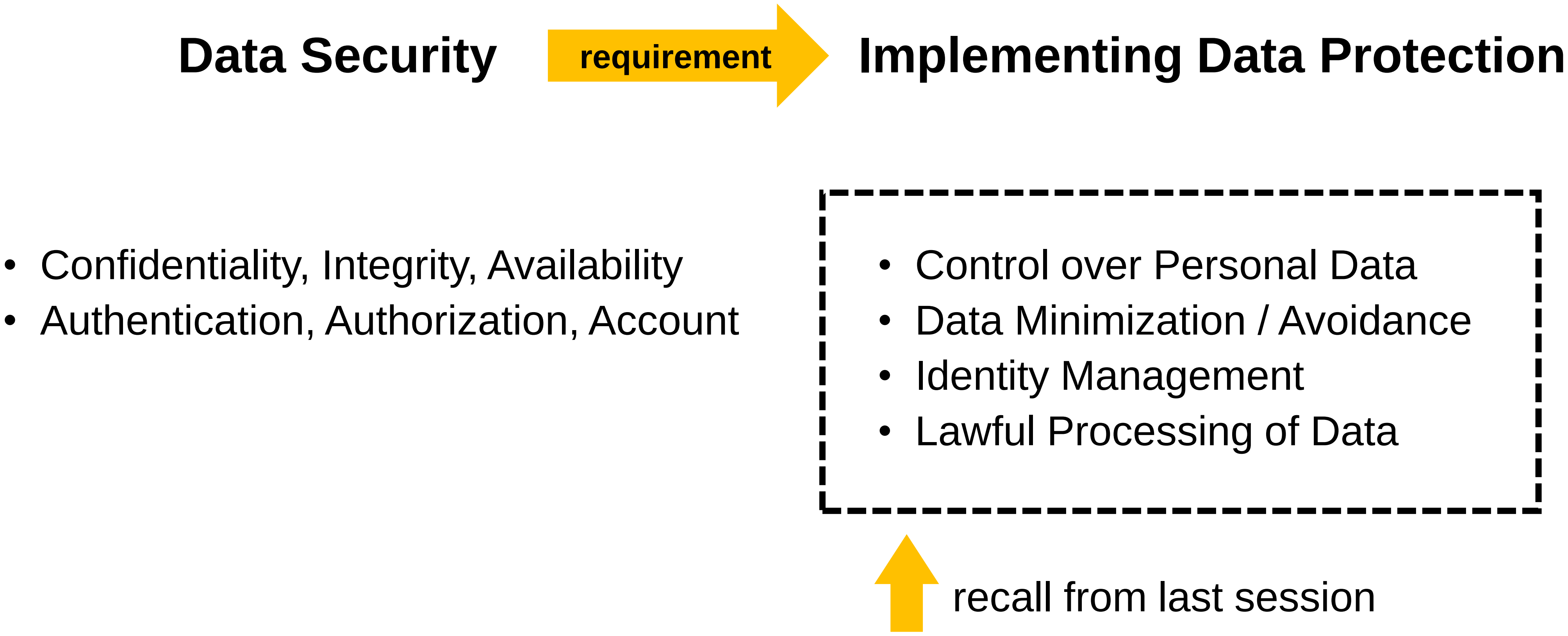
- Authentication
- Authorization
- Accounting




THE CRYPTO NUT:
MY DATA IS SAFE BEHIND SIX LAYERS OF SYMMETRIC AND PUBLIC-KEY ALGORITHMS.
WHAT DATA IS IT?
MOSTLY ME EMAILING WITH PEOPLE ABOUT CRYPTOGRAPHY.

https://www.xkcd.com/1269/

Technical Means for Securing Data



Data Security

requirement

Implementing Data Protection

- Confidentiality, Integrity, Availability
- Authentication, Authorization, Account

- Control over Personal Data
- Data Minimization / Avoidance
- Identity Management
- Lawful Processing of Data

recall from last session

Privacy Enhancing Technologies

Have Objectives:

- Control over Personal Data

Transparency

- Lawful Processing of Data

- Data Minimization / Avoidance

- Data Security and Integrity

- Identity Management

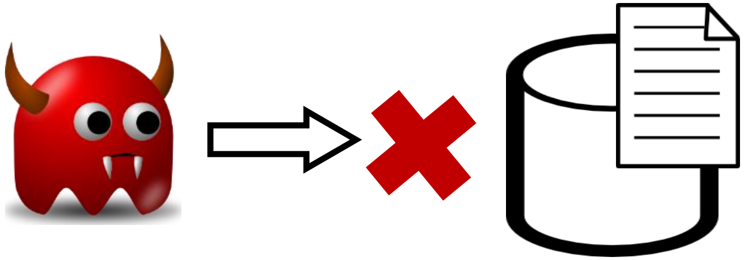
THE CRYPTO NUT:
MY DATA IS SAFE BEHIND SIX LAYERS OF SYMMETRIC AND PUBLIC-KEY ALGORITHMS.
WHAT DATA IS IT?
MOSTLY ME EMAILING WITH PEOPLE ABOUT CRYPTOGRAPHY.

https://www.xkcd.com/1269/

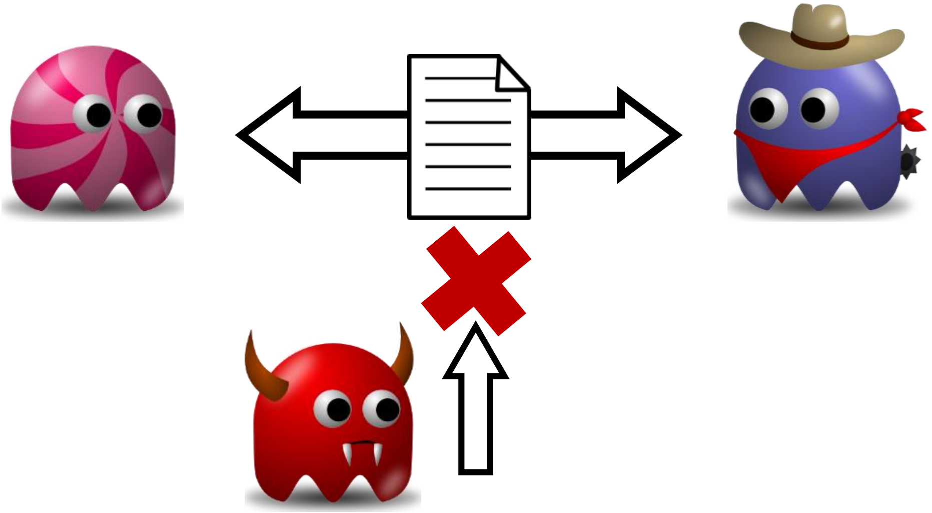
Confidentiality

- Information NOT available or disclosed to unauthorized parties

- Stored Data



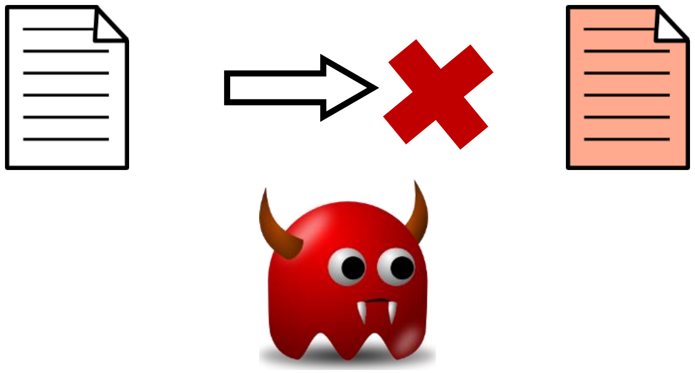
- Data in Transit



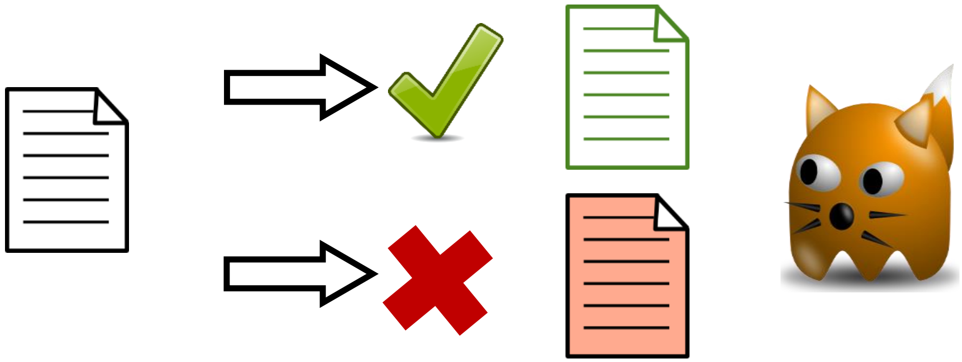
Integrity

- Information NOT modified by unauthorized parties or in an unauthorized manner

- Unauthorized Parties



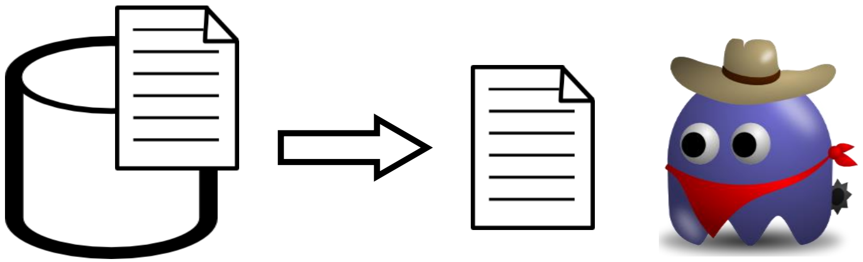
- Unauthorized Manner



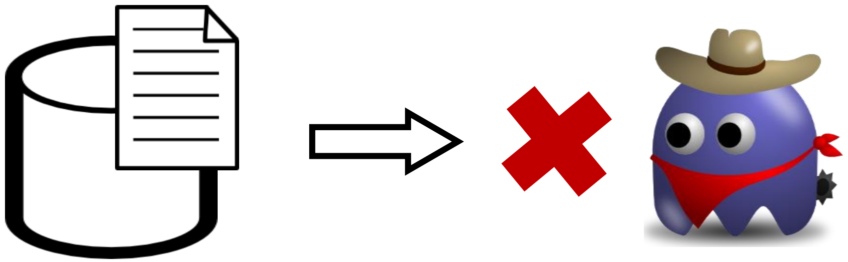
Availability

- Information available when needed

- Available



- NOT Available

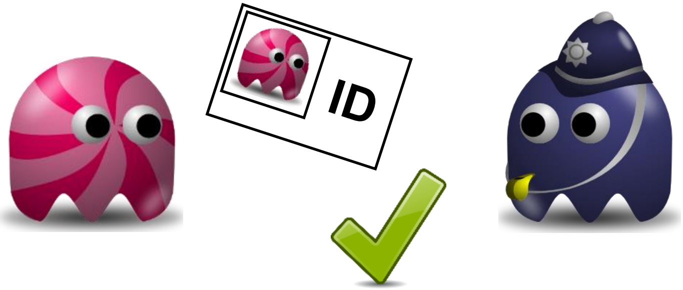


Authentication

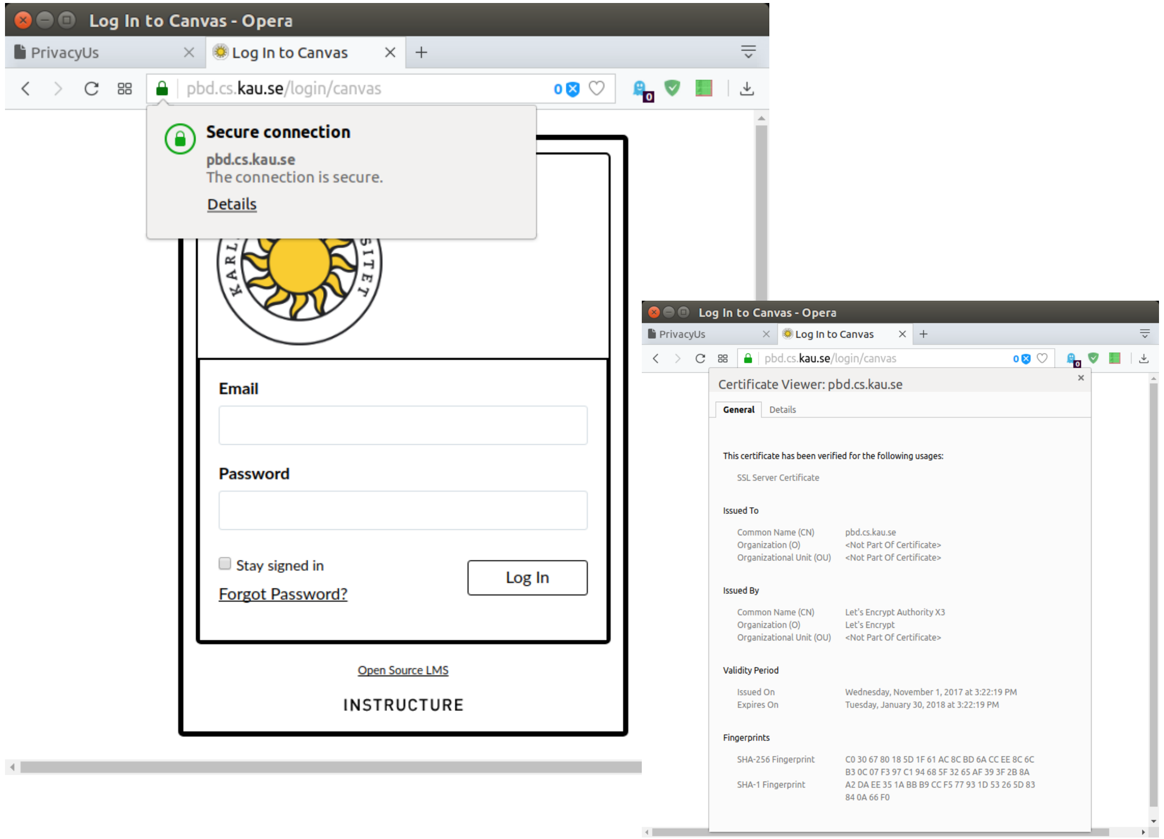
- Assurance of an identity claim

Are you really who you claim to be?

- ID cards



- Digital certificates



Secure connection

pbd.cs.kau.se

The connection is secure.

Certificate Viewer: pbd.cs.kau.se

This certificate has been verified for the following usages:

SSL Server Certificate

Issued To

Common Name (CN)	pbd.cs.kau.se
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>

Issued By

Common Name (CN)	Let's Encrypt Authority X3
Organization (O)	Let's Encrypt
Organizational Unit (OU)	<Not Part Of Certificate>

Validity Period

Issued On	Wednesday, November 1, 2017 at 3:22:19 PM
Expires On	Tuesday, January 30, 2018 at 3:22:19 PM

Fingerprints

SHA-256 Fingerprint	C0 30 67 80 18 5D 1F 61 AC 8C BD 6A CC EE 8C 6C B3 0C 07 F3 97 C1 94 68 5F 32 65 AF 39 3F 2B 8A
SHA-1 Fingerprint	A2 DA EE 35 1A BB B9 CC F5 77 93 1D 53 26 5D 83 84 0A 66 F0

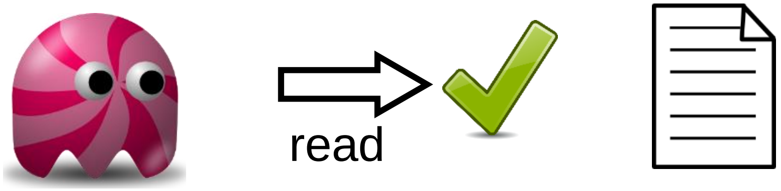
Authorization

- Grant or deny access to resources

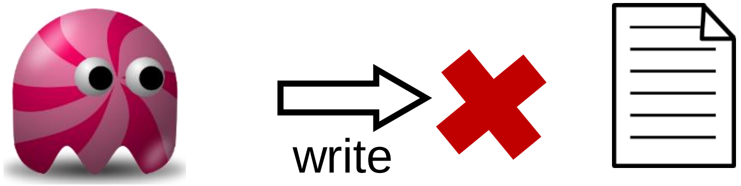
  operations over resources

(once authenticated)

- Authorized



- NOT Authorized

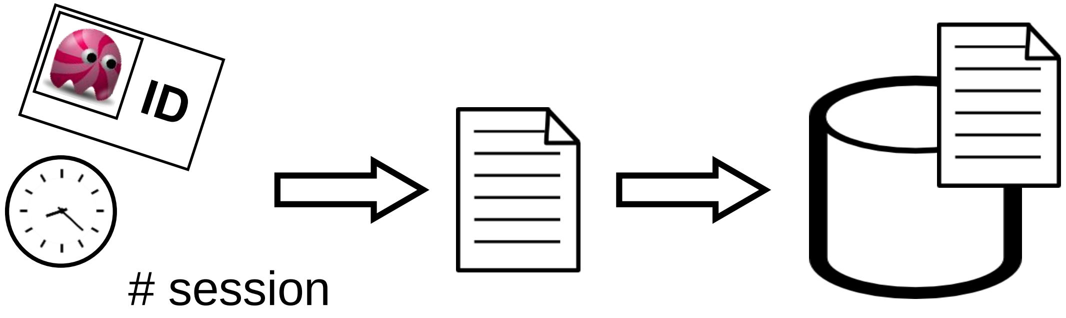


Accounting

- Keeping track of information

  users and data

- Building and storing log data



Part 1: Introduction

- What are PETs?
- Security technologies
- Why we need technologies

next session

- Pfitzmann & Hansen terminology