

# PRISM

## Privacy-Aware Secure Network Monitoring

---

Giuseppe Bianchi

PRISM Project Technical project coordinator  
CNIT / Univ. Roma Tor Vergata



# network monitoring is a must...

---

- performance
  - Operate & manage network
  - Understand/improve network dynamics
- Security and safety
  - Of the network infrastructure
  - Of the citizens and for public interest
- Regulation
  - Enforce security-concerned laws (anti-terrorism, etc)
    - Data Retention
    - Lawful Interception
    - ...



# ... but it may be also a threat

---

- Against users' privacy
  - Infringement of data protection laws
- Profiling and wiretapping abuses
  - Even by highly reputed national operators
    - 4+ recent "cases" from late 2006
- Measurement data misuse
  - "*The only difference between Internet measurement research and hacking is intent*"  
[quote from A. Braidó]

***The right to privacy: a current EU priority***



# Regulation and network monitoring

---

- Network Monitoring: deals with information which IS, to all extents, personal data

**personal data** = “any information relating to an identified or identifiable natural person (*identification: directly or indirectly*)”  
[Directive 95/46/EC]

“... [ISPs] will have to treat all IP information as personal data to be on the safe side...”  
[opinion WP136 4/2007]

- Should be carried out in line with rules and limitations set by data protection
  - used only for the original specified purpose;
  - adequate, relevant and not excessive to purpose;
  - kept secure and destroyed after its purpose is fulfilled;
  - ...
- AND must cope with traffic logging provisions
  - Data retention obligations
    - Directive 2006/24/EC, national directives/implementations





# PRISM challenge

---

- Regulation says:
  - Data should be used only for the original specified purpose
- Hardly followed in practice
  - Data first collected, (almost) regardless of purpose
  - Typical answer: *"I don't strictly need now this data, but I might need, hence I must (!) collect it"*
- Challenge: engineer a system which
  - Guarantees network customers' privacy
    - by technically preventing data analyses which are out of purpose
  - Meanwhile retaining flexibility
    - Purpose and depth-level of data analysis may change in short time (e.g. under an attack)

Breaking false dichotomy: **MUST** trade privacy for utility/security

---



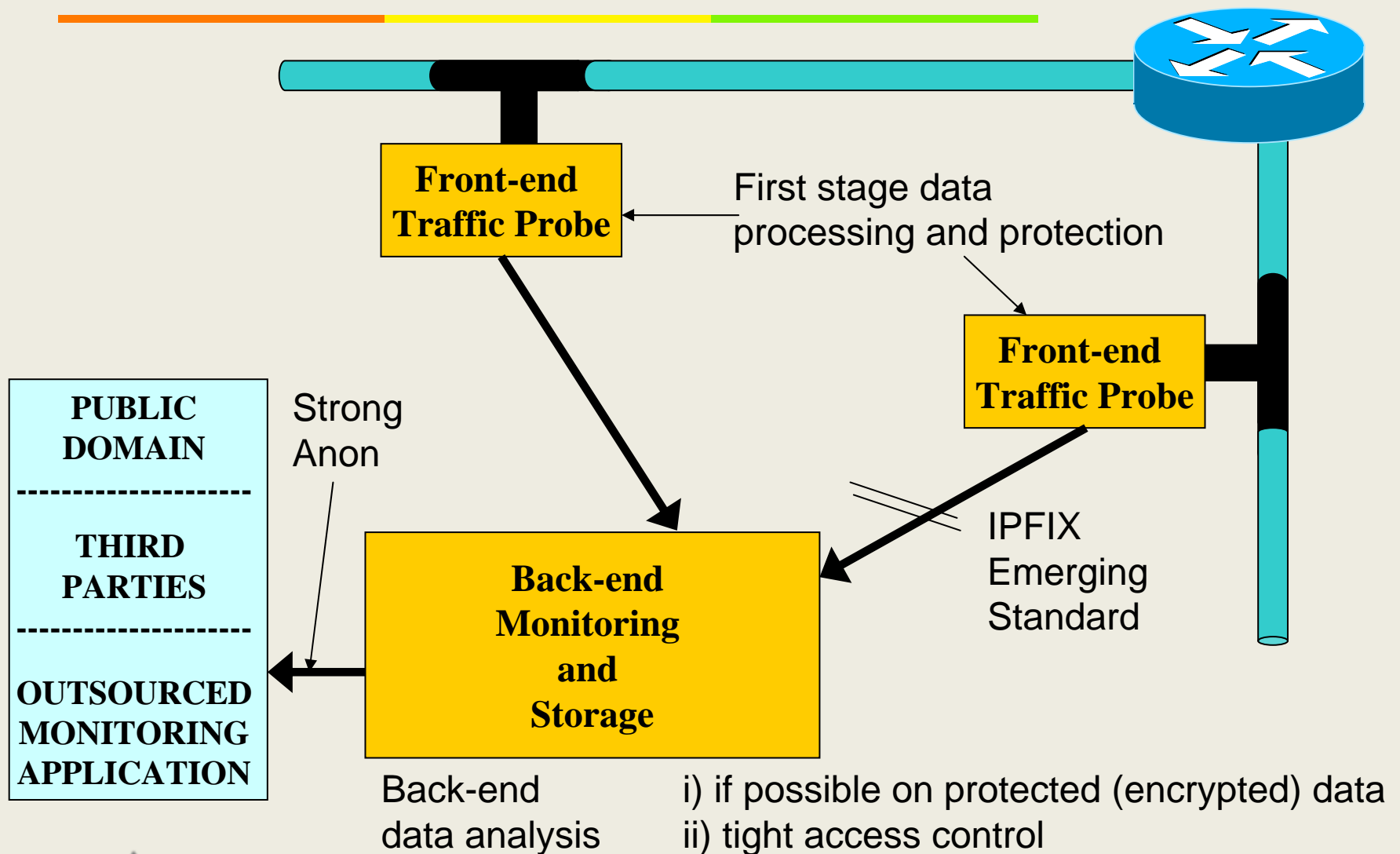
# Is this “only” a researchers’ vision?

---

- No: it’s coming (even against data controller’s wish)
- Evolution fostered by EU strong attention towards data protection
- Italy in first line - example: jan 17, 2008, technical/organizational measures to protect/handle retained electronic data
  - Example of provisions set forth (subset):
    - severe restrictions (including sysadm) on the access to the data
      - to be eventually implemented via biometric approaches;
    - Access restrictions to storage locations
      - Need to deploy sophisticated authorization systems
      - rigid separation between personnel/entity which assigns authorization credentials, and personnel/entities which shall access the data
    - Audit logs for operating personnel’s access traceability
    - Separate storage
      - data retained for investigation purposes and fraud detection/repression
      - Versus data used by ordinary O&M (billing, statistics, etc.)
    - Mandatory cryptographic protection of retained data
    - ...



# PRISM approach: two-tiered



# Why two-tiers? Flow segregation!

---



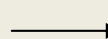
Lots of information; not useful;



**Front-end  
Traffic Probe**

Filter out flows with certain properties

- Suspected of anomaly
- Requiring accounting
- etc



metadata

Filter out information not needed for further processing

## PROS:

- **Performance**: scalability, reduced back-end processing and storage requirements
- **Privacy**: only flows that require to be monitored are delivered; purpose enters into play.

## (PAST) CHALLENGE:

- Is this type of processing feasible on the front-end? **YES!**
- 



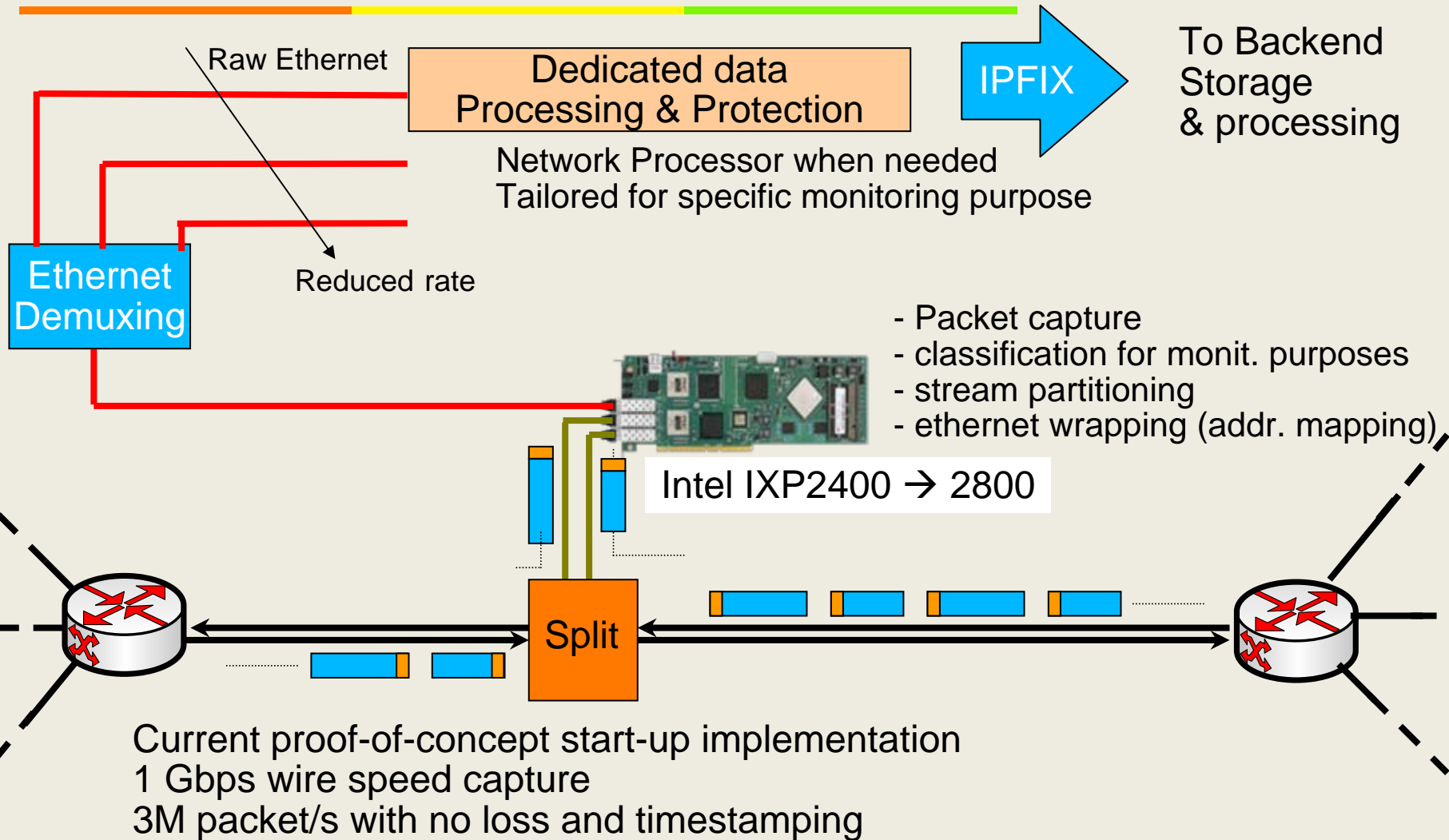
# Boosting Front-end processing

---

- Efficient data structures, trading efficiency with deterministic operation
  - Match
    - Traditional Bloom Filters or similar structures
  - Count
    - Counting Bloom filters with Conservative Update
  - Scan
    - Variation detector (new in PRISM!)
  - Rate Control
    - Probabilistic/approximate Token Buckets (new in PRISM!)
  - Approximate State Machine
    - Bloom-filter based (in progress)
- Our initial conclusion: front-end can efficiently embed a LOT more capabilities than what initially expected



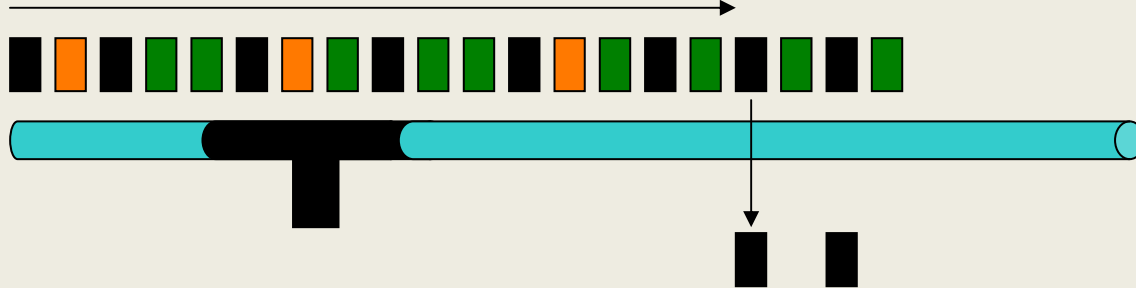
# Front-end Technology



# Limit of “plain” segregation

---

Front-End Processing in progress



Anomaly detected: Flow delivered  
... but past activity lost!  
... past activity could be now essential!!

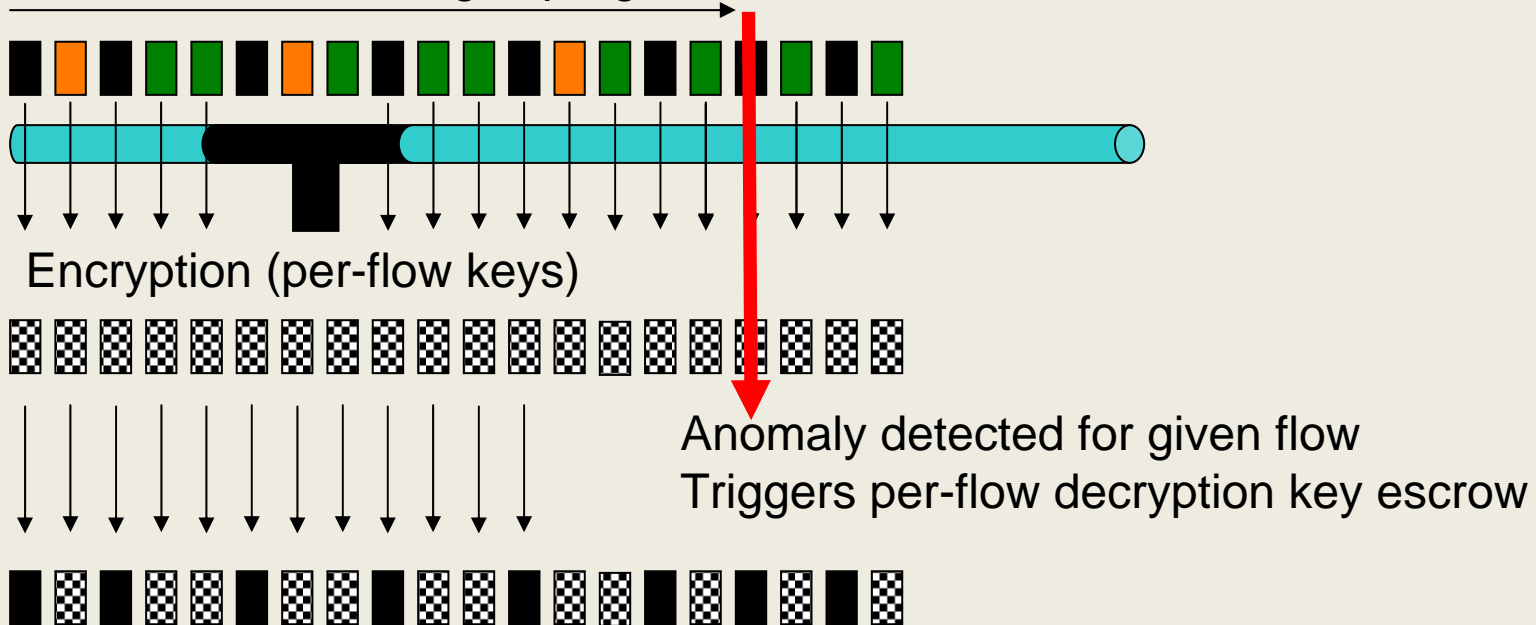
Need to go “back in time” in some specific applications.  
HOW TO?



# Encryption and escrow mechanisms

IDEA: bind per-flow decryption to the occurrence of some measurement related conditions

Front-End Processing in progress



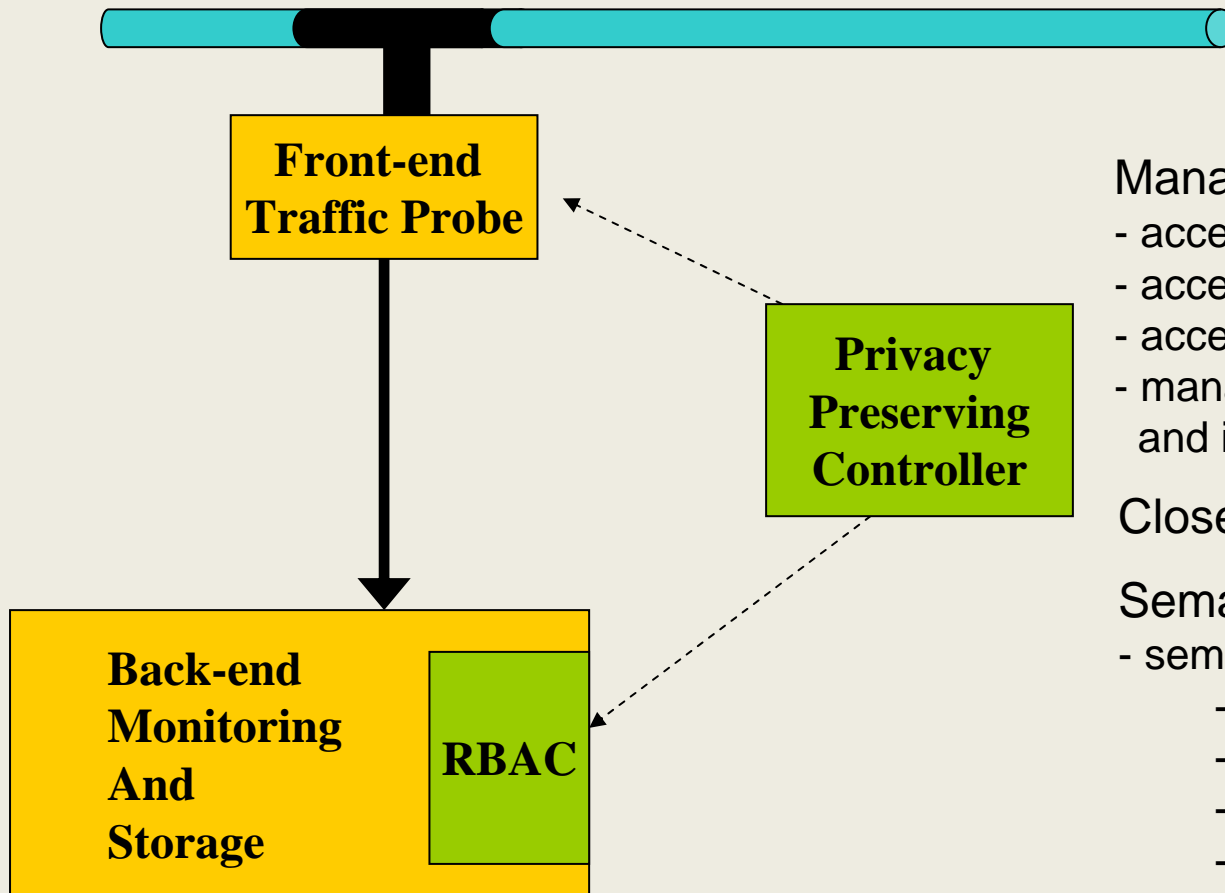
Issues addressed:

- 1) escrow after multiple conditions occur
- 2) fast search on encrypted traces



# Managing the system

---



Manages Authorization Framework

- access to stored data
- access to front-end facilities
- access to data analysis procedures
- manages crypto keys (if needed and if not solved by prior approach)

Closely remembers a PMI

Semantic approach under spec.

- semantically describe:
  - Monitoring apps and primitives
  - Their purpose
  - The specific data they operate on
  - the privacy level of the data
  - the applicable regulation
  - the role of end users



# Status of PRISM's workplan

---

- Two-tiered approach
  - right direction
- Front-end processing
  - good solutions
- Data export Protocols
  - IPFIX with Anonymization support under standardization
- Applications
  - traffic and anomaly OK
  - signature-based IDS/IPS next challenge
- System architecture
  - ideas OK but detailed specification in progress
- Front-end implementation
  - Started, promising results and performance with NP
- Back-end specification
  - started
- Semantic approach
  - initial ideas

