


Project SSPDDP

https://www.sspddp.nl

Today's program

14:00 Welcome and Introduction by Marc Stevens & Ryan Bulthuis

14:10 Presentation of WP3: "Policy-modelling and enforcement"

14:45 Presentation of WP1: "Security, Trust and Privacy"

15:10 Break

15:20 Presentation of WP2: "Scalability distributed Big Data"

15:45 General discussion

16:05 Closing


Project SSPDDP

https://www.sspddp.nl

Project SSPDDP

- Secure
  - Cryptographic mechanisms for Immutability, Privacy, & Trust management
- Scalable
  - Enable resource restricted clients
  - High-performance accelerators for high throughput & low latency
- Policy-enforced
  - Augment smart contracts with formal modelling of business and legal policy
  - Design business processes to enforce policy compliance
- Distributed Data Processing
  - Information sharing and processing across organizations

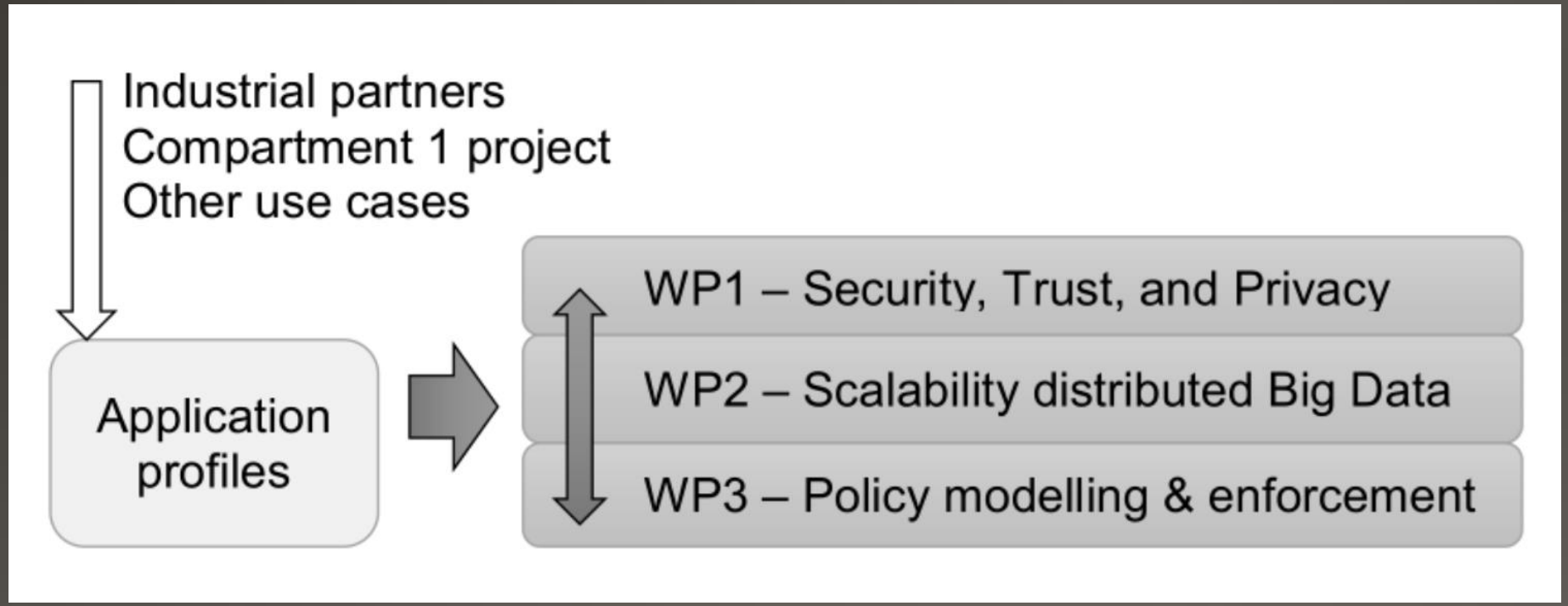
People

- Investigators
  - Marc Stevens (CWI) (PI, Sec L)
  - Tijs van der Storm (CWI)
  - Tom van Engers (UvA) (Pol L)
  - Sander Klous (UvA)
  - Cees de Laat (UvA)
  - Henri Bal (VU) (Sca L)

  - Yurry Hendriks (ABN AMRO)
  - Ryan Bulthuis (ABN AMRO)
  - Leon Gommans (AirFrance-KLM)
  - Peter van den Hoven (ING)
  - Tommy Koens (ING)

- Funded Researchers
  - Aron van Baarsen
    - 4y PhD on Sec @ CWI
    - Started 1 March 2020
  - L. Thomas van Binsbergen
    - 2+y Postdoc on Pol @ CWI
    - Started 15 June 2019
  - Lu-Chi Liu
    - 4y PhD on Pol @ Uva
    - Started 1 July 2019
  - Marc X. Makkes
    - 3y postdoc on Sca @ VU
    - Started 1 November 2018
- Affiliated researchers
  - Giovanni Sileno (postdoc @ UvA)
  - Esteban Landerreche (PhD @ CWI)

Project overview



WP1 Status

"Security, trust and privacy"

- Timestamping and Blockchain immutability from computational hardness (non-PoW)
- Short cryptographic proofs of predicates
- Cryptographic mechanisms to share data privately
- Identity management, authentication and authorization

- 4y PhD, Aron van Baarsen, 1-3-2020
- (PhD, Esteban Landerreche)

Research output:

- *Non-interactive Cryptographic Timestamping based on Verifiable Delay Functions*, Financial Crypto 2020
- *On Immutability of Blockchains*, ERCIM Workshop 2018

WP2 Status

"Scalability distributed Big Data"

- Reduced resource requirements for blockchain clients
- Blockchain bootstrapping mechanism
- High performance cryptographic primitives for accelerators

- Postdoc, Mark Makkes, 1-11-2018
  (On other project: April-Sep)

Research output:

- "*Dietcoin: hardening Bitcoin transaction verification process for mobile devices"*, VLDB'19

WP3 Status

"Policy modelling & enforcement"

- Co-creation of DM-policy
- DM-policy compliant data-transaction agreement creation mechanism
- Policy Simulation Environment
- Compliance enforcement mechanism
- Reporting and dispute settlement mechanism

- PhD, Lu Liu, 1-7-'19
- Postdoc, Thomas van Binsbergen, 15-6-'19

Research output:

- *Purely Functional GLL Parsing*, Journal Computer Languages, 2020
- *eFLINT - An action-based language for reasoning about norms*, ICT.Open, 2020
- Demo eFLINT

Usecase: KYC

- Required by WWFT law
  (Wet ter voorkoming van witwassen en financieren van terrorisme)

- Know your costumer concerns the discipline of getting to know the customer: both legal entities and natural persons.
- In general, KYC is carried out on a case-by-case basis:
  - A number of data points are collected and the ownership trail is identified up to an ultimate beneficial owner (UBO).
  - A (typically automated) risk assessment is carried out.
  - The outcome determines whether or not a bank will commence business, exit a client or take mitigating measures (e.g. annual review cycle).

- Issues
  - Rapidly increasing costs
  - Duplication of efforts across financial institutions
  - Suboptimal effectiveness of decentralized activities

- Opportunity for cooperation & Benefits
  - Customer experience
  - Efficiency
  - Effectivity
  - Reputation

- As a result, proof of concepts have readily identified a number of topics around which further research may prove beneficial:
  - Security
  - Ownership (of data and policy)
  - Privacy (GDPR)
  - Competition limitations (for NL: Autoriteit Consument en Markt)

KYC Explained: Drivers and Limitations

- **Main driver:**
- WWFT

- **Limiting factors / constraints:**
- Privacy law (GDPR)
- Competition law
- Internal policies and risk appetite

- **Goal**
- Share data for KYC processes
- Ability to run decentralized specialty models (risk calculations)

- **Min requirement to solution**
- Auditability of information: quality, changes, flows
- Compliant with legal limitations

Issues:

- High **duplication of manual efforts** in data collection and processing
- Individual banks have an **incomplete view** on customer behaviour / alerting function lacks
- **Variation in WWFT interpretation** and KYC requirements
- **Decentral processing** with limited possibility for alignment