ITASEC20
ITALIAN CONFERENCE ON CYBERSECURITY

GDPR Compliance Through Authorization Systems

Said Daoudagh

Ph.D. Program in Computer Science CICLO XXXIII
said.daoudagh@{isti.cnr.it, di.unipi.it}

The Problem

The General Data Protection Regulation (GDPR) requires that the controller and the processor need to:
(1) demonstrate the compliance with the GDPR - "Accountability" principle;
(2) demonstrate the appropriate technical security level - "integrity and confidentiality";
(3) adapt and rethink their data practices so as to be aligned with the "data protection by-design and by-default" approach (Art. 25).

SMEs Needs

Being (by-design) compliant with the GDPR means having solutions that:
(1) are general-purpose;
(2) must take in consideration the regulation by-design;
(3) must be easily integrated with the existing business processes; and finally
(4) must be rooted in the GDPR principles dictated in Art. 5.

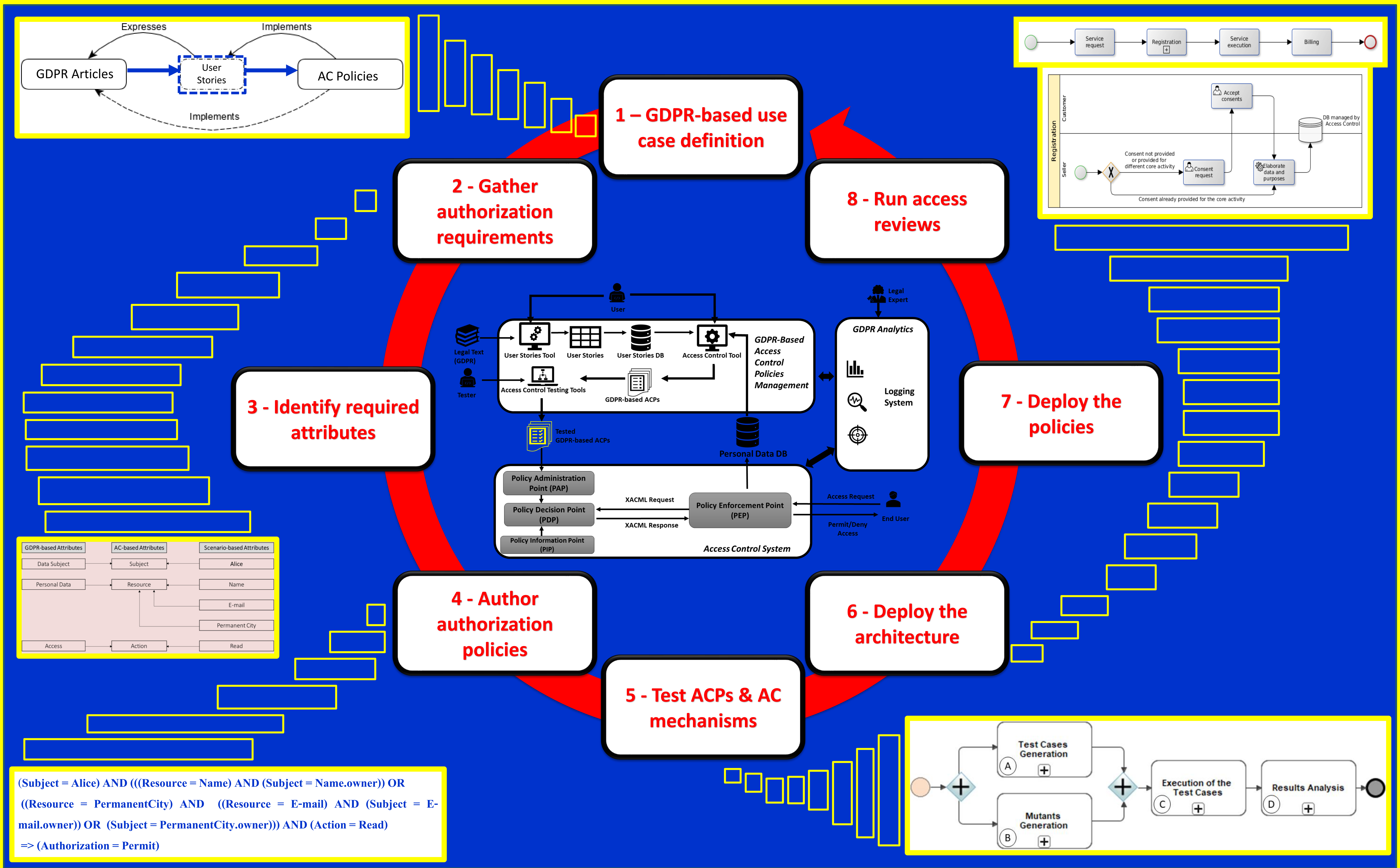
Limits of Existing Solutions

Different works are trying to give an answer on how to comply with the GDPR

- but most of them are in a early stage;
- lack of automation and tools supporting their proposal in real scenarios.

Seminal works are:
[6] discusses a systematic approach for implementing Access Control Policies (ACPs) in an industrial setting, but without taking in consideration any legal framework;
[10] presents an approach to extract ACPs from the Data Protection Directive (Directive 95/46/EC in force before the GDPR).

Main Ideas and Results



(Subject = Alice) AND (((Resource = Name) AND (Subject = Name.owner)) OR ((Resource = PermanentCity) AND ((Resource = E-mail)) AND (Subject = E-mail.owner)) OR (Subject = PermanentCity.owner))) AND (Action = Read)
=> (Authorization = Permit)

References

[1] Cesare Bartolini, Said Daoudagh, Gabriele Lenzini, and Eda Marchetti. *GDPR-Based User Stories in the Access Control Perspective*. In Proc of QUATIC, 2019.
[2] Cesare Bartolini, Said Daoudagh, Gabriele Lenzini, and Eda Marchetti. *Towards a Lawful Authorized Access: A Preliminary GDPR-based Authorized Access*. In Proc. of ICSOFT, 2019.
[3] Aantonia Bertolino, Said Daoudagh, Francesca Lonetti, and Eda Marchetti. *XACMUT: XACML 2.0 Mutants Generator*. In Proc. of Mutation 2013..
[4] Antonia Bertolino, Said Daoudagh, Francesca Lonetti, and Eda Marchetti. *An Automated Model-based Test Oracle for Access Control Systems*. In AST, 2018
[5] Antonia Bertolino, Said Daoudagh, Francesca Lonetti, Eda Marchetti, and Louis Schilders. *Automated testing of eXtensible Access Control Markup Language-based access control systems*. IET Software 7, 4 (2013).
[6] David Brossard, Gerry Gebel, and Mark Berg. *A Systematic Approach to Implementing ABAC*. In Proc. of the 2Nd ACM ABAC, 2017.
[7] Antonello Calabrò, Said Daoudagh, and Eda Marchetti. *Integrating Access Control and Business Process for GDPR Compliance: A Preliminary Study*. In Proc. of ITASEC, 2019.
[8] Said Daoudagh, Francesca Lonetti, and Eda Marchetti. *XACMET: XACML Modeling & Testing*. Software Quality Journal (2019). In Press.
[9] Said Daoudagh and Eda Marchetti. *A Life Cycle for Authorization Systems Development in the GDPR Perspective*. In ITASEC, 2020.
[10] Kaniz Fatema, Christophe Debruyne, Dave Lewis, Declan O'Sullivan, John P. Morrison, and Abdullah-Al Mazed. *A Semi-Automated Methodology for Extracting Access Control Rules from the European Data Protection Directive*. In IEEE SP Workshops, 2016.

Take Home Message

KEEP
CALM
AND
COMPLY WITH
THE GDPR

PhD Researcher: Said Daoudagh
Supervisor: Dr. Eda Marchetti (ISTI-CNR)
Co-Supervisor: Dr. Anna Monreale (UniPi)
Internal Committee:
Prof. Gabriele Lenzini (SnT-UniLu)
Prof. Laura Ricci (UniPi)

http://pages.di.unipi.it/daoudagh/gdpr-access-control