SPECIAL

Scalable Policy-awarE Linked Data arChitecture for prIvacy, trAnsparency and compLiance

Deliverable D5.4

Public challenge report V2

Document version: 1.0

SPECIAL DELIVERABLE

Name, title and organisation of the scientific representative of the project's coordinator:

Ms. Jessica Michel t: +33 4 97 15 53 06 f: +33 4 92 38 78 22 e: jessica.michel@ercim.eu

GEIE ERCIM, 2004, route des Lucioles, Sophia Antipolis, 06410 Biot, France

Project website address: http://www.specialprivacy.eu/

Project	
Grant Agreement number	731601
Project acronym:	SPECIAL
Project title:	Scalable Policy-awarE Linked Data arChitecture for prIvacy, trAnsparency and compLiance
Funding Scheme:	Research & Innovation Action (RIA)
Date of latest version of DoW against which the assessment will be made:	17/10/2016
Document	
Period covered:	M22-M30
Deliverable number:	D5.4
Deliverable title	Public challenge report V2
Contractual Date of Delivery:	30-06-2019
Actual Date of Delivery:	29-07-2019
Editor (s):	Uroš Milošević (TF)
Author (s):	Uroš Milošević (TF), Wouter Dullaert (TF)
Reviewer (s):	Rigo Wenning (ERCIM), Eva Schlehahn (ULD)
Participant(s):	
Work package no.:	5
Work package title:	Use Case Implementation & Evaluation
Work package leader:	TR
Distribution:	PU
Version/Revision:	1.0
Draft/Final:	Final
Total number of pages (including cover):	28

Disclaimer

This document contains description of the Scalable Policy-awarE Linked Data arChitecture for prIvacy, trAnsparency and compLiance (SPECIAL) project work and findings.

The authors of this document have taken any available measure in order for its content to be accurate, consistent and lawful. However, neither the project consortium as a whole nor the individual partners that implicitly or explicitly participated in the creation and publication of this document hold any responsibility for actions that might occur as a result of using its content.

This publication has been produced with the assistance of the European Union. The content of this publication is the sole responsibility of the SPECIAL consortium and can in no way be taken to reflect the views of the European Union.

The European Union is established in accordance with the Treaty on European Union (Maastricht). There are currently 28 Member States of the Union. It is based on the European Communities and the Member States cooperation in the fields of Common Foreign and Security Policy and Justice and Home Affairs. The five main institutions of the European Union are the European Parliament, the Council of Ministers, the European Commission, the Court of Justice and the Court of Auditors (http://europa.eu/).

SPECIAL has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 731601.

Table of Contents

1 Introduction

Driven by use case scenarios, WP5 aims to evaluate the results obtained in WP2 (Policy and Transparency Framework), WP3 (Big Data Policy Engine), and WP4 (User Interaction) under real-world conditions. More specifically, the goal of T5.3 Public challenges is to expose the developed system and its components to public hacking challenges, which would, together with the internal backend scalability and robustness testing performed in WP3 (D3.3 and D3.5) and frontend testing in WP4 (D4.2 and D4.4), provide the necessary feedback for further development of the SPECIAL platform.

In D5.2 Public Challenge Report V1, we explained that in order to guarantee the robustness of our architecture, such challenges must focus on ensuring that both the individual components and the infrastructure as a whole are capable of sharing data only with authorized parties, while guaranteeing that policies and regulations are being adhered to. We also argued that this means involving other aspects of the system, be it technical or legal, highlighting any limitations. This is worth repeating as the outcome of the three rounds of challenges has made us reconsider and adapt our strategy, as we will explain further below.

1.1 Deliverable scope

This deliverable discusses the technical, legal, and practical requirements considered with the goal of running the public hacking challenge program and maximizing its outcome. It gives an overview of the carried out SPECIAL public challenge, the accompanying program policy (provided in the Annex of this document), the dissemination activities, and the program results. Finally, it discusses the follow-up action, namely the public challenge workshop organized at a BDV PPP event to collect on-site feedback from different groups of participants.

2 Challenge scope

The SPECIAL public challenges were envisioned with the goal of learning about any shortcomings of the SPECIAL platform that could result in a data breach or a violated data usage policy. Such shortcoming could include bugs pertaining to authentication/authorization, the APIs or other bugs related to data flows, the logs or log formats, the front-ends, or even the policy language. Any tests would cover only what is directly within SPECIAL's span of control (that is, being developed by the project partners) and not involve third party solutions, be it commercial or open-source. Moreover, any known flaws in the system would be also made public and excluded from the challenge scope.

More specifically, we hereby explicitly list what was defined as in and out of scope of the official SPECIAL Public Challenge (Table 1).

In-scope platform components	***Out of scope platform components***
• *Integrated system as a whole* • *Compliance engine* • *Consent management front-end(s)* • *Transparency & compliance front-end(s)* • *Usage policy language* • *Policy log vocabulary*	• Apache Kafka • RethinkDB • Keycloak • HermiT • Any other components not built and maintained by the SPECIAL Consortium

Table 1: In and out of scope platform components

2.1 Attacks and vulnerabilities

Similarly, we confined both possible attacks and vulnerabilities to a clearly defined list to achieve the desired outcome and avoid potential misinterpretations of the policy or abuse of the public challenge program.

Table 2 lists what we considered as qualifying and non-qualifying vulnerabilities and attacks.

Qualifying attacks & vulnerabilities	***Non-qualifying attacks & vulnerabilities***
• *Authentication vulnerabilities* • *Privilege escalation* • *Significant Security Misconfiguration* • *Information Disclosure* • *Injection vulnerabilities*	• Clickjacking • Denial of service attacks • Phishing attacks • Social engineering attacks • Content spoofing • Issues requiring direct physical access • Flaws affecting out-of-date browsers and

	plugins • Weak password policies • HTTP 404 codes/pages or other HTTP non-200 codes/pages

Table 2: Qualifying and non-qualifying attacks and vulnerabilities

2.2 Use cases

Although inspired by the three pilots, the public challenges were never meant to happen in live setups involving real data subjects. Moreover, due to the sensitivity of the information, business and security concerns, disclosing the details on the real-world setups of the pilots partners was also not an option. For this reason, the participants were offered a simulated environment, running on synthesized data, without direct references to the pilot partners or their use cases.

2.2.1 Fictional use case “BeFit”

To avoid potential business, security and legal obstacles, the platform setup was based on BeFit, a fictional use case. In this scenario, a fitness tracking application collects personal data, such as physical characteristics and workout activity, for different commercial purposes.

The BeFit scenario covers all aspects of the current architecture – consent management per user, compliance checking, and transparency for both the data controller and the data subject. In addition to this, the setup was accompanied by a log generator for synthesizing application processing events.

3 Challenge conditions

Participation in the SPECIAL Public Challenge was made entirely voluntary. All participants were expected to have read and agreed to the official challenge terms and conditions to be eligible for any challenge benefits. The SPECIAL Consortium, however, reserved the right to change or modify the terms of the program at any time.

3.1 Ground Rules

To ensure healthy competition and desired challenge outcome, but also prevent abuse, we set forth some ground rules for all participants:

- All participants should aways research and disclose bugs and vulnerabilities in good faith.
- No participant should ever leave any system or its components in a more vulnerable state than they found it.
- No participant should ever publicly disclose a vulnerability without the SPECIAL Consortium's consent, unless the vulnerability has already been disclosed by the SPECIAL Consortium.

3.2 Eligibility to Participate

For the sake of fairness, we also ensured all challenge participants met the challenge eligibility criteria. Namely, the participants had to:

- Not be directly affiliated with SPECIAL or any of the project partners.
- Not be in violation of any law or regulation with respect to any activities directly or indirectly related to the SPECIAL Public Challenge and the involvement must not be an infringement of any law or regulation for SPECIAL or its project partners (e.g. export regulations).

Not meeting the above eligibility criteria or breaching these Terms in any other way would give us the right to, in our sole discretion, remove the participant from the SPECIAL Public Challenge and disqualify them from receiving any benefit of the SPECIAL Public Challenge.

3.3 Personal Data

Participation in the challenge was not conditioned on providing any personal data. Nevertheless, to qualify for any benefits of the challenge, the participants were required to share the data necessary for processing vulnerability reports and paying out bounties. The SPECIAL Consortium would never collect more than what is requested of the participants for these purposes, and any redundant data would be deleted on receipt.

4 Process

4.1 Testing environment

Due to the nature of the challenge and the resources at the Consortium's disposal, an adequate shared testing environment would have been considerably more difficult to provide than a dedicated setup per challenge participant. Our solution was to offer preconfigured installation packages representing different real-world scenarios inspired by our pilot use cases. This allowed the platform to be deployed and tested locally or on any remote server under the participant's control. Additionally, the policy language could be tested outside the platform setup.

For ease of deployment, the fictional use case was provided as a dedicated installation package (i.e. a Docker container image) and distributed via a public repository – the official project GitHub repository[1].

4.2 Communication

Building further on the principle of responsible disclosure, we ensured all communication between the participant reporting a system flaw and the public challenge committee would be private until the reported flaw has been fixed. To this end, the SPECIAL consortium set up a dedicated e-mail address for such reports.

4.2.1 Report

Once a participant has identified a vulnerability, they would be expected to prepare a comprehensive report and send it to the challenge committee for assessment. If the committee would find the report valid, the participant would be awarded points, based on the severity level of the finding (Section 4.3.1).

A "comprehensive report" was expected to include at least:

- A detailed description of the vulnerability;
- Steps (or a proof-of-concept) used to expose the vulnerability;
- Specific source code references (when possible; the report would have to at least list the relevant architecture components).
- Any other relevant information.

4.3 Format and timing

As a dedicated budget for the public challenge was not foreseen by the project plan, a traditional continuous bug bounty program, guaranteeing a financial reward per reported vulnerability was not

[1] https://github.com/specialprivacy/demonstrator

feasible. Therefore, the SPECIAL public challenge needed to explore alternative approaches, such as gamification, to provide enough incentives for long-term participation.

Our chosen strategy was to award points for each report (rather than a financial incentive), which could be then aggregated per participant and ranked. The motive behind introducing a leaderboard was threefold:

- Creating a sense of community,
- Eliciting the desire to participate and compete, and
- Paying out bounties at the end of the challenge to the top-ranking competitors, rather than every time a participant reports a vulnerability.

To further incentivize participation over a longer period of time, the challenge program was organized into three runs. During each of the runs, the participants were given three months to examine the system and look for flaws.

4.3.1 Scoring, ranking, and rewards

The more convincing the demonstration of breaking defined policies and compliance rules or otherwise highlighting limitations of our system or its parts, the more points would be awarded to the participant.

The SPECIAL Consortium had the right to determine the level of severity based on a number of criteria, including the CVSS score (Section **Error! Reference source not found.**), decide if the minimum severity threshold is met, and assess whether the vulnerability was previously reported.

4.3.1.1 Scoring system

The Common Vulnerability Scoring System (CVSS)[2] provides a way to capture the principal characteristics of a vulnerability, and produce a numerical score reflecting its severity, which can then be translated into a qualitative representation (such as low, medium, and high).

The CVSS score would allow us to formalize the severity levels and assign points based on a predefined policy. A sample challenge scoring system is given in Table 3.

Severity level	*Low*	*Medium*	*High*
Points	5	10	15

Table 3: Scoring system

Once a vulnerability has been confirmed, the competitor would be assigned the number of points they were due, which would then be added to their total and published along with other participants' scores on a dedicated challenge page. The information would be limited to the chosen or assigned (if not provided) competitor alias, the number of reports, and the total score (Table 4). The total score would determine the overall ranking.

[2] https://www.first.org/cvss/

POSITION	ALIAS	NUMBER OF REPORTED VULNERABILITIES			SCORE
		Low	Medium	High	

Table 4: Ranking table structure

The details of all confirmed issues would be given on a separate page, providing full transparency, while also allowing all participants to inform themselves on the already resolved vulnerabilities before starting their investigation.

4.3.1.2 Rewards

Any rewards would be based on the above described public score granted entirely at the discretion of the SPECIAL Consortium. To qualify for points under the SPECIAL public challenge program, the competitor would have to:

- Be the first to report a vulnerability;
- Disclose the vulnerability report directly and exclusively to the SPECIAL public challenge committee.

DTAG offered to provide six mobile devices (three high-end and three mid-range phones) as rewards. TF would complement this with 3 Amazon vouchers of € 50, allowing us to offer three rewards per run. The partners committed to delivering the prizes to the top 3 contributors within 30 days of a completed 3-month run. (The SPECIAL Consortium, however, reserved the right to change the aforementioned rewards without prior notice.)

5 Promotion

5.1 Target audience

The SPECIAL Public Challenge was advertised as an open call to researchers, ethical hackers, and IT professionals, but also any other individuals who would be interested in testing and inspecting the SPECIAL platform for security vulnerabilities, bugs or flaws in the system or its components. Due to the nature of the technologies involved, basic knowledge of semantic web technologies was desirable, but not mandatory, as the intention was to target all aspects of the system.

5.2 Channels

To reach out to the desired audience, we used all dissemination channels established in WP 6 and at our disposal. More specifically, this meant at least informing the public via our website, the social media, the universities and research projects we collaborate with, and the BDV PPP. A more detailed overview of these channels is given in Table 5.

Channel type	***Channel***
Website	• SPECIAL website
Social media	• Twitter – project and partner profiles • LinkedIn – partner pages and profiles • Meetup – BigData.be community
Academic community	• Wirtschaftsuniversität Wien, Austria • Technische Universität Berlin, Germany • Università degli Studi di Napoli Federico II, Italy • Katholieke Universiteit Leuven, Belgium (via TenForce)
Partner projects	• RestAssured[3] • ReCRED[4] • MyHealthMyData[5] • SODA[6] • DECODE[7]
Other	• BDV PPP newsletter and website • DPVCG W3C community group

Table 5: Dissemination channels

[3] https://restassuredh2020.eu

[4] https://www.recred.eu

[5] http://www.myhealthmydata.eu

[6] https://www.soda-project.eu

[7] https://decodeproject.eu

6 Outcome

After almost a year of actively advertising the public challenge via the available channels, despite implementing all the risk mitigation measures foreseen by the work plan, the SPECIAL consortium has not received any vulnerability reports. Given the amount of promotion that was put in via the different dissemination means, our belief is that it is highly improbable the message did not reach the intended audience. More likely possibilities would be that:

1. No vulnerabilities were found (perhaps, because the solution relies on many industry standards, such as those used for authentication and authorization);
2. The potential participants did not find the prize pool motivating enough given the required effort to find a vulnerability.

Some of the feedback received via Twitter seems to suggest the latter (Figure 1). It is also worth noting that, in hope of increasing the challenge exposure, SPECIAL has explored alternative platforms for running the program, such as HackerOne[8], which provides access to the largest global ethical hacker community. Unfortunately, even though the SPECIAL platform qualifies for the Community Edition[9] of the platform, after several meetings with the company representatives the consortium was unable to provide the necessary financial guarantees for the success of the program. In other words, the representatives insisted that, for a challenge to be successful, the size of the prize pool must be directly correlated with the effort that is expected from the community. (As the service is hosted by HackerOne, and the company earns commissions from transactions, it is also in its interest that even open-source projects meet certain requirements that can increase the program's chance of success.) For these reasons, we are inclined to believe that the challenge outcome is a direct result of the aforementioned lack of a dedicated budget for rewards.

Figure 1. Target audience feedback received via Twitter

[8] https://www.hackerone.com

[9] https://www.hackerone.com/product/community

7 Public challenge workshop

As the outcome of the originally envisioned SPECIAL public challenge did not yield the expected result after the first two runs, despite our best efforts, we made a timely decision to reconsider our approach to collecting the required feedback from the community. This decision was also made in line with our earlier plans to also put other aspects of the system to the test, including the legal choices, as well as the business ones. An opportunity was identified at the annual BDV PPP Summit held June 26-28, 2019, in Riga, Latvia.

The BDV PPP Summit[10] is a major EU event aimed at driving European innovation in Big Data and Artificial Intelligence. Key European industry, academia and policy-making players gather every year to foster cross-sector collaboration and shape strategies for European leadership in Big Data and data-driven Artificial Intelligence. The Summit welcomes the hundreds of organizations involved in the Big Data Public Private Partnership, as well as all those who want to be part of the European Big Data Ecosystem. The first day of the 2019 Summit delivered the BDV PPP Conference, with keynotes, speeches and discussion panels focused on Big Data, AI, and Privacy. The conference was followed by two days of parallel thematic workshops as part of the BDV PPP Meetup, the BDVA General Assembly and the Big Data Value PPP Steering Committee.

Within the BDV PPP Meetup, SPECIAL was provided with an opportunity to organize an on-site public challenge in the form of a workshop[11].

7.1 Workshop format

The workshop, titled "*Public Challenge: Looking for flaws in the SPECIAL platform*", started with an introductory presentation giving an overview of the SPECIAL project, goals, challenges, use cases, and results. The consortium members put an emphasis on the SPECIAL Platform and its components, explaining the technical choices, but also the legal and business aspects of the proposed solutions. The introductory session was then followed by a participant-driven brainstorming session, organized in a Carousel/Graffiti format.

[10] http://www.bdva.eu/node/1246

[11] https://www.big-data-value.eu/ppp-summit-2019/program-2019/

Figure 2. SPECIAL public challenge workshop, introduction

Carousel Brainstorming is often used as a cooperative learning activity both to discover and discuss background knowledge prior to studying a new topic, as well as for reviewing already learned content.[12] In such a setup, participants are organized in small groups which rotate around the room, stopping at various "stations" for a designated period of time. At each of the stations, the groups answer questions, solve problems, discuss a topic, or provide feedback on questions, problems, or topics or problems placed on "graffiti" walls. Each group posts their ideas on the graffiti wall for all groups to read, then, after an allotted period of time, participants rotate to another graffiti wall in the room and follow the same process.

To cover all aforementioned aspects of the system, and ensure valuable contributions from participants with different backgrounds, the workshop was organized around three graffiti walls, corresponding to three key themes:

- **Performance and Scalability**, addressing any technical or other flaws that could considerably affect the performance and scalability of the overall architecture or its components;
- **Privacy and Security**, targeting any issues that could lead to a data breach, a violated data usage policy, or in some other way jeopardize the integrity of the system or the processed data;
- **Business Value**, aimed at any flaws that could hamper the applicability of the setup, diminish its value, or the value of the impacted line of business applications in real-world scenarios, considering costs, ROI, or other relevant business factors.

The ten workshop participants were split into three groups: two teams of three and one team of four participants. Each of the groups had at least some knowledge of each of the themes, and each station was further assigned one SPECIAL consortium representative for clarifications and assistance. (It is worth noting, however, that the consortium representatives did not interfere in the brainstorming process.)

[12] Santa, C., & Havens, L. (1995). Creating independence through student-owned strategies: Project CRISS. Dubuque, IA: Kendall-Hunt.

Figure 3. SPECIAL public challenge workshop, brainstorming process

Every round (Figure 3) would begin with the SPECIAL consortium representative explaining the theme of the station and providing a summary of the ideas already on the wall, if any, in no more than two minutes. The groups would then spend three minutes brainstorming and writing down their thoughts (using sticky notes). Finally, the teams would discuss the proposed ideas and questions for five minutes, while the SPECIAL consortium representative would attempt to cluster similar ideas together. Each group would then move on to the next station.

Figure 4. SPECIAL public challenge workshop, brainstorming

7.2 Workshop outcome

The outcome of the three rounds of workshop brainstorming is close to one hundred sticky notes, spread across fifteen possible clusters. As the collected notes overlap (often across themes) and vary in terms of context and quality, representing not only participants' remarks, but also concerns, ideas for improvement, and even general comments, we hereby summarize the feedback and list the most common/valuable questions and ideas. We do not attempt to address them here (some of them have already been addressed in other deliverables), but will use them for guidance and fine tuning of the platform as we approach its final release (D3.6), as well as for future work beyond the lifetime of the project.

7.2.1 Performance and Scalability

The performance and scalability discussions revolved around the integration of the platform in existing infrastructures and the added overhead, distribution of the architecture to multiple controllers, unexpected downtime and resilience, environmental factors, and updating the system on the fly:

1. How soon before the SPECIAL platform affects the user experience in applications processing personal data?
2. How would the SPECIAL platform affect the system as a whole?
3. How would the platform scale with respect to the number of controllers?
4. How would the system deal with power outages?
5. How would the deployment choices (cloud vs. on-premise, container vs. native) affect the performance?
6. Some existing infrastructures come with considerable network overhead.
7. What about other effects of the existing infrastructure?
8. How does the context of processing (e.g. different industries) affect the performance?
9. To what extent can different needs of different stakeholders affect the performance?
10. What about interoperability?
11. Can the platform deal with more complex or granular policies?
12. How do you keep all technologies/components up to date?
13. The law can change. How do you update the system in case of legislative changes?
14. Will it scale with an increase on the demand side (velocity and variety)?

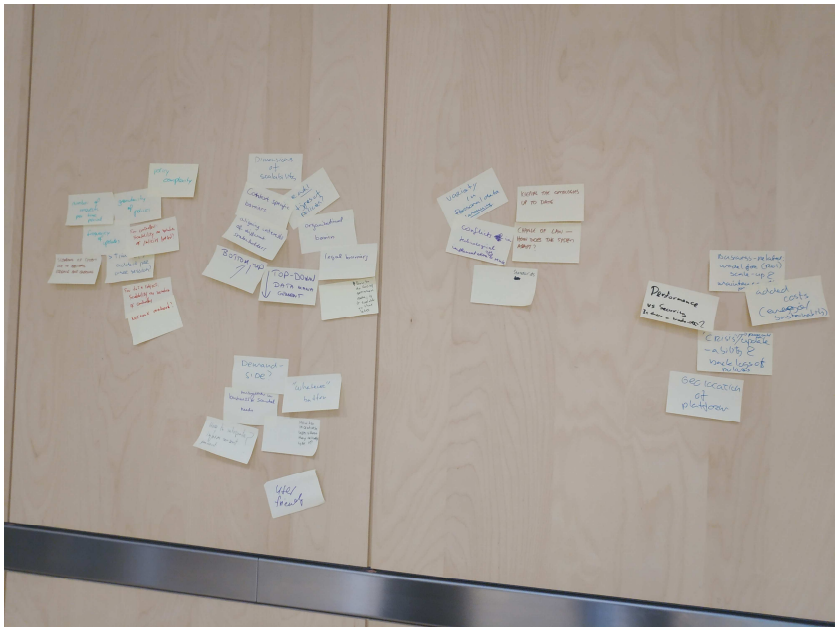


Figure 5. SPECIAL Public challenge workshop, Performance & Scalability station

7.2.2 Privacy & Security

The privacy and security questions and ideas were mostly aimed at the data protection measures, risk management, usability aspects, governance of the data and the processing applications, incident management, legal requirements, and cross-border data sharing:

1. Are the current technical choices enough as data breach protection measures?
2. What happens on the controller's side if the platform is not available?
3. What happens on the data subject's side if the platform is not available?
4. There is a data inventory, but perhaps you also need a data processing application inventory?
5. Does the platform provide breach notifications?
6. Are the policies expressive enough to satisfy the users' actual preferences?
7. What does the controller need to do? What should they not do?
8. What if the controller/processor is malicious?
9. Can the platform guarantee it is tamper-proof?
10. Some data subjects will be less technology-proficient.
11. What about touchless interfaces (e.g. speech)?
12. How do you deal with organizations that lack (people with) the necessary expertise?
13. Is the setup enough for a data protection impact assessment?
14. People do not always act in their best interest.
15. Is automatic compliance checking legally enough? The legal landscape is also volatile.
16. What about cross-border data sharing and different legal requirements in different countries?

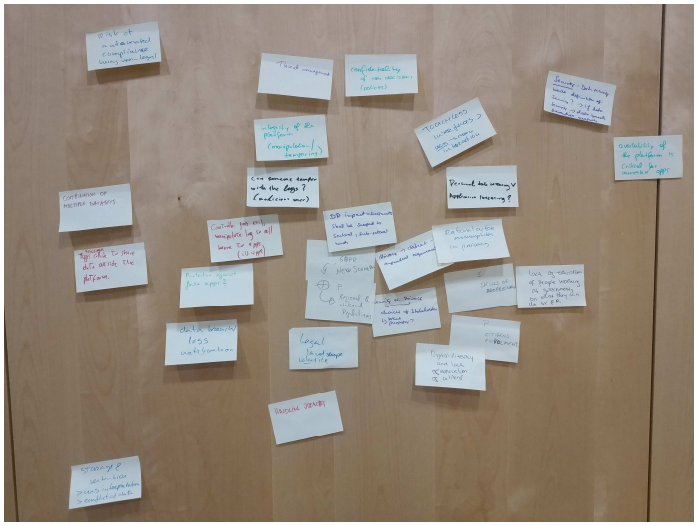


Figure 6. SPECIAL Public challenge workshop, Privacy & Security station

7.2.3 Business Value

The business value discussions focused on the added costs of the system, the trade-offs between the legal requirements and business priorities, the market segments and the target customers, the usability and other requirements for market penetration, as well as the alternative solutions:

1. How do you deal with the cognitive limitations of the data controller/processor/subject?
2. Some companies might not want that much increase in transparency.
3. Who is really the target group - the data subject or the service provider?
4. How do you prioritize business issues?
5. Is detailed, formal, policy specification too much overhead for the data subject? What about the controller?
6. How do you incentivise the data subject to use the system?
7. How much cost does it (i.e. integration and maintenance) add to the overall system?
8. Can the platform actually help businesses demonstrate compliance?
9. Can you ever prevent secondary use?
10. What do you do with conflicting policies?
11. Which sectors should the consortium target?
12. Does it have the same value for all sectors?
13. The platform needs to be made integrable and interoperable with many applications.
14. Why should a company choose this solution over another one?

Figure 7. SPECIAL Public challenge workshop, Business Value station

8 Conclusion

This deliverable gave an overview of the defined requirements and scope of the SPECIAL public challenge, as well as the plan and the carried-out activities. The challenge call for entries and the accompanying program policy (available in the Annex) were published on our website,[13] and actively promoted using all available channels throughout the duration of the challenge. However, as the call failed to attract the desired target audience (most likely due to a lack of a dedicated budget for the rewards program), the consortium opted for an alternative approach to collecting public feedback.

A SPECIAL public challenge workshop was organized on-site at the 2019 BDV PPP Summit, where we sought to address a more diverse audience, rather than just Big Data and cybersecurity professionals and enthusiasts, and gather input from the participants on other aspects of the SPECIAL platform and our technical choices. The workshop was organized around three themes: Performance and Scalability, Privacy and Security, and Business Value. The gathered feedback suggests the platform could be improved with respect to aspects such as integration with existing infrastructure, data governance, platform resilience, and incident management before its final release (D3.6). Other topics, such as distribution of the architecture across controllers, updating the system on the fly, catering for users of different ICT skill levels, or the market approach, requires further research and development which are out of the scope of SPECIAL, but provide fertile ground for future work.

[13] https://www.specialprivacy.eu/platform/public-challenge

9 Annex: Public challenge call for entries and program policy

Discover security vulnerabilities, bugs or flaws in the system or its components, and win interesting prizes!

What is SPECIAL?

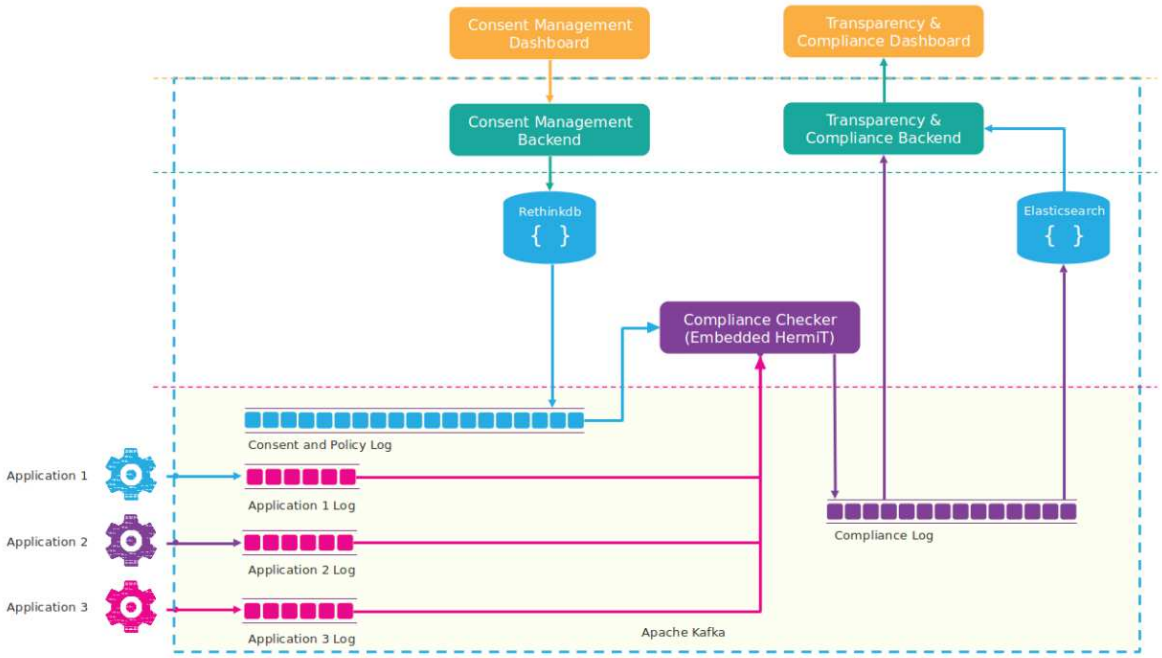
The SPECIAL project[14] addresses the contradiction between Big Data innovation and privacy-aware data protection by proposing a technical solution that makes both of these goals realistic. SPECIAL allows citizens and organisations to share more data, while guaranteeing data protection compliance, thus enabling both trust and the creation of valuable new insights from shared data. We develop technology which:

- supports the acquisition of user consent at collection time and the recording of both data and metadata (consent policies, event data, context) according to legislative and user-specified policies;
- caters for privacy-aware, secure workflows which include usage/access control, transparency and compliance verification;
- aims to be robust in terms of performance, scalability and security, all of which are necessary to support privacy preserving innovation in Big Data environments; and
- provides a dashboard with feedback and control features which make privacy in Big Data comprehensible and manageable for data subjects, controllers, and processors.

SPECIAL Platform

The SPECIAL platform is an extensible environment for managing personal data usage policies, ensuring compliance with such policies, and tracking personal data usage along with the context it is being used in. The high-level overview of this policy-aware Linked Data architecture and engine is given below:

[14] The project "Scalable Policy-awarE Linked Data arChitecture for prIvacy, trAnsparency and compliance" (SPECIAL) has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No No. 731601.



A demo video is available here[15]. For a detailed description of the system and its components, we strongly recommend consulting at least:

- Deliverable 3.2 - Policy & events release (M16)[16]

Other relevant project deliverables are also public and can be found here[17]. Additionally, we also suggest reading about:

- The SPECIAL Usage Policy Language[18]
- The SPECIAL Policy Log Vocabulary[19]

What is the SPECIAL Public Challenge?

The SPECIAL Public Challenge is an open call to researchers, ethical hackers, IT professionals and other interested individuals to test and inspect the SPECIAL platform and point out any security vulnerabilities, bugs or flaws in the system or its components.

[15] https://www.specialprivacy.eu/images/videos/ESWC%20demo%20submssion.mp4

[16] https://www.specialprivacy.eu/images/documents/SPECIAL_D3.2_M16_V1.0.pdf

[17] https://www.specialprivacy.eu/publications/public-deliverables

[18] https://aic.ai.wu.ac.at/qadlod/policyLanguage/

[19] https://aic.ai.wu.ac.at/qadlod/policyLog/

"I am not familiar with some of the technologies. Can I still participate?"

Basic knowledge of semantic web technologies (OWL, RDF, reasoning engines) is desirable, but not mandatory. There are many other ways you can contribute. Please see the description of the program scope below.

Scope

We are interested in learning about any shortcomings of the SPECIAL platform that could result in a data breach or a violated data usage policy. Examples of such shortcoming could include bugs pertaining to authentication/authorization, the APIs or other bugs related to data flows, the logs or log formats, the front-ends, the policy language, etc. The platform can be deployed and tested locally or on any remote server under your control. Additionally, the policy language can be tested outside the platform setup.

Note: This is an early prototype of what is expected to reach TRL5[20] by 2020. It is, therefore, not production ready.

Below, we describe what is in and out of scope of our Public Challenge program.

In-scope platform components

- Integrated system as a whole
- Compliance engine (but not HermiT itself)
- Consent management front-end(s)
- Transparency & compliance front-end(s)
- Usage policy language
- Policy log vocabulary

Out of scope platform components

- Apache Kafka
- RethinkDB
- Keycloak
- HermiT
- Any other components not built and maintained by the SPECIAL Consortium

Qualifying attacks & vulnerabilities

[20] https://en.wikipedia.org/wiki/Technology_readiness_level

- Authentication vulnerabilities
- Privilege escalation
- Significant Security Misconfiguration
- Information Disclosure
- Injection vulnerabilities

Non-qualifying attacks & vulnerabilities

- Clickjacking
- Denial of service attacks
- Phishing attacks
- Social engineering attacks
- Content spoofing
- Issues requiring direct physical access
- Flaws affecting out-of-date browsers and plugins
- Weak password policies
- HTTP 404 codes/pages or other HTTP non-200 codes/pages

Process

The process is simple. The challenge program is organized into three 3-month runs, with the last one ending on May 31, 2019. During each of the runs, you get as much time as you want to examine the system and look for flaws. Any time you find something you consider worth mentioning, you prepare a comprehensive report and send it to us for assessment. If we find the report valid, we will immediately reward you with points, based on the severity level of the finding. (Please see 'Rewards' below.)

How do I report security issues?

Please send all your findings to special-bugs@ercim.eu, including:

- A detailed description of the vulnerability;
- Steps (or a proof-of-concept) used to expose the vulnerability;
- Specific source code references (when possible; you should at least list the relevant architecture components).
- Any other relevant information.

Rewards

Rewards are based on a public score granted entirely at the discretion of the SPECIAL Consortium. To qualify for points under this program, you should:

- Be the first to report a vulnerability;
- Disclose the vulnerability report directly and exclusively to us, unless the vulnerability has already been disclosed by us.

Severity assessment

The more convincing the demonstration of breaking defined policies and compliance rules or otherwise highlighting limitations of our system or its parts, the more points you get. The SPECIAL Consortium reserves the right to determine the level of severity (based on a number of criteria, including the CVSS score), decide if the minimum severity threshold is met, and assess whether the vulnerability was previously reported.

Severity level	Low	Medium	High
Points	5	10	15

Ranking

The first time your report is resolved and closed, your name or chosen alias will be added to our public “Thank you” scoreboard. (Please see ‘Personal data’ for additional information.) For that and every subsequent report, the awarded points will be added to your total score. The total number of accumulated “Thank you” points will determine the participant ranking at the end of the run. The top-3 contributors at the end of each run will get rewards!

This run's bounties

The prizes will be sent out to the top 3 contributors within 30 days of a completed 3-month run. The SPECIAL Consortium reserves the right to change any of the below awards without prior notice.

1st place	A high-end smartphone
2nd place	A mid-range smartphone
3rd place	A € 50 Amazon voucher

Terms

Participation in the SPECIAL Public Challenge is entirely voluntary. By submitting a report, you are indicating that you have read and agree to our Terms, as outlined below. The SPECIAL Consortium reserves the right to change or modify the terms of this program at any time.

Ground Rules

- Always research and disclose in good faith.
- Never leave any system in a more vulnerable state than you found it.
- Never publicly disclose a vulnerability without our consent.

Eligibility to Participate

To be eligible to participate in our Public Challenge, you must:

- Not be directly affiliated with SPECIAL or any of the project partners.
- Not be in violation of any law or regulation with respect to any activities directly or indirectly related to the SPECIAL Public Challenge and the involvement must not be an infringement of any law or regulation for SPECIAL or its project partners (e.g. export regulations).

Not meeting the above eligibility criteria or breaching these Terms in any other way gives us the right to, in our sole discretion, remove you from the SPECIAL Public Challenge and disqualify you from receiving any benefit of the SPECIAL Public Challenge.

Personal Data

Please keep in mind that we do not require any personal data apart from what we believe is absolutely necessary for processing vulnerability reports and paying out bounties. We will never ask for more than this. Should you ever disclose more than what is requested of you, we will erase such data on receipt.

As a privacy project SPECIAL allows anonymous or pseudonymous (alias) submissions to be processed for conducting the hacking challenge. Contact data are however greatly appreciated for questions and getting back to you. Your name or alias will be publicly displayed on the scoreboard. To hand out prizes to winners these will be asked their name and address for shipment as well as a confirmation that the prize has been received. Depending on the regulatory framework of the partner donating the prize in question the the latter information may be necessary to be stored with their financial information for audit-purposes. Contact information of the contributors will be deleted at latest three month after the SPECIAL project has ended.

You have the right to access your personal data processed by us. You may withdraw your consent to process your personal data – your contributions will then be handled as anonymous or under an alias of your choice.

Getting started

We offer preconfigured installation packages representing different real-world scenarios inspired by our pilot use cases.

BeFit

This is the default package. In this scenario, a fitness tracking application collects personal data, such as physical characteristics and workout activity, for different commercial purposes. It comes with a simple UI for consent management per user, a log generator for synthesizing application processing events, and a transparency and compliance dashboard.

You will find everything you need to get started in our official GitHub repository.

Questions?

Feel free to drop us an e-mail at special-bugs@ercim.eu