BehavAuth

Human behaviour based authentication for Internet of Things

Open Call Project for TagItSmart: Grant agreement 688061

WP2: D2.3 Impact and dissemination activities report

Deliverable ID:	**D 2.3**
Deliverable Title:	**Impact and Dissemination activities report**
Revision #:	**1.0**
Dissemination Level:	**Public**
Responsible beneficiary:	QBE
Contributing beneficiaries:	All
Contractual date of delivery:	28/02/2018
Actual submission date:	1/3/2018

Start Date of the Project: 1 September 2017 Duration: 6 Months

European Commission

Contents

Section 1 - Introduction and impact ***5***

Section 2 - Co-creation activities ***7***

2.1 Engaging psychologists **7**

2.2 Engaging privacy experts **8**

2.2.1 Digital catapult 8

2.2.2 GDPR Seminar – Penningtons Manches LLP 9

2.3 Potential customers **10**

2.4 End-users **11**

Section 3 - On-line dissemination activities ***13***

3.1 Micro-website **13**

3.2 Social media **16**

3.3 Press release **16**

3.4 Scientific dissemination **16**

Section 4 - Events – MeetUps – Conferences ***17***

4.1 Open calls kick-off meeting (Vaasa, Finland) **17**

4.2 ICT Proposers Day 2017 (Budapest, Hungary) **18**

4.3 Santander Breakthrough Event (Guildford, UK) **19**

4.4 GDPR Seminar (Basingstoke, UK) **19**

4.5 SETSquared Club meeting (Guildford, UK) **20**

4.6 MeetUp Internet of Things (Guildford, UK) **20**

Section 5 - Conclusion ***21***

Section 6 - References ***22***

Document history

Revision	Date	Modification	Authors
0.1	28/02/2017	Final version ready for review	N. Palaghias

Introduction

The main objective of this document is to provide the information related to the dissemination activities performed on behalf of the BehavAuth and TagItSmart projects as well as the impact achieved.

Section 1 provides an introduction to the deliverable about the impact and dissemination activities achieved during the BehavAuth project. A brief summary of the dissemination activities is provided at the beginning of the section. Following, the impact of the BehavAuth project is described in various sectors such as benefits towards the SMEs as well as the wider, social, environmental and regional impact that the project will achieve in long-term.

In **Section 2**, an analysis of the co-creational activities performed throughout the whole duration of the project in order to shape the use cases and requirements of the project based on the stakeholder engagement. The main stakeholders of the project are psychologists, privacy experts, end-users and potential customers. Each category of the stakeholders was engaged from the beginning of the project in order to shape the use cases and the requirements of the project. The activities performed to engage each stakeholder category are detailed and analysed in this section, as well as discussing the input and feedback received from the stakeholders.

Next, **Section 3** describes the actions taken from the BehavAuth project in order to on-line disseminate the BehavAuth and TagItSmart projects. The on-line dissemination activities include the design and development of an on-line micro-website that is co-hosted at Quadible's web-presence website, dissemination activities through social media, press releases and scientific publications. Each one of the dissemination activities are detailed in a separate subsection describing the actions and the activities performed.

Given the overview of the impact and the dissemination activities, the co-creational activities and the on-line dissemination activities, **Section 4** provides an analysis of the events, conference and meetups that the BehavAuth team attended to disseminate the project and promote the adoption of TagItSmart and BehavAuth. Each event, conference and meetup is described individually as well as discussing the potential outcome received from each event.

Finally, this deliverable ends with the conclusion provided in **Section 5**.

Section 1 - Introduction and impact

BehavAuth started from day one to disseminate the project. From the first stages of the project, the web-presence of the BehavAuth was established by developing and publishing a micro-website hosted on Quadible's website and by engaging through social media. Quadible attended the kick-off meeting of the project and other events. Furthermore, Quadible hosted a plethora of meetings with potential end-users and customers not only to understand their needs, but also to prepare them to become early adopters.

Dissemination at a glance. Initially this section will describe the actions performed from the beginning of the BehavAuth project to increase its impact. At the beginning of the project Quadible created a micro-website at http://www.quadible.co.uk/behavauth in order to spread the word and to establish the web presence of the project. Quadible's daily website traffic allowed the information of our daily visitors to learn and understand the concept of the BehavAuth and the TagItSmart projects. In parallel, Quadible initiated the stakeholder engagement from the beginning of the project in order to define the use cases and derive the functional requirements of the system. The stakeholder engagement included the initiation of collaboration with end-users, potential customers, psychologists and privacy experts. Each stakeholder provided their insights and knowledge for us to shape the requirements of the platform. Quadible has initiated the dissemination of the BehavAuth project and the TagItSmart project through social media such as Facebook, Twitter and LinkedIn. The existing social media accounts of Quadible and its teams' individuals, have been used in order to post a) updates about the project, b) updates in the cyber security area and in particular in the authentication field including biometrics.
Quadible has attended various events in order to disseminate the work from the beginning of the project and also to maximise the impact of the BehavAuth project as well as the TagItSmart project. Some of the events that Quadible attended as part of the BehavAuth project are TagItSmart kick-off meeting, SETSquared Club meeting, ICT Proposers Day 2017 and Santander Breakthrough Event.

Benefits for SMEs. While SMEs strive to develop, and bring to the market innovative ideas that they have captured, they confront some barriers that speed down the process and drain their resources. Amongst these barriers is the lack of the appropriate infrastructure to develop their business ideas. TagItSmart provides a platform that will enable SMEs to create innovative solutions leveraging information data from all the production circle of a product and behavioural data provided by the consumer.
BehavAuth strengthens the benefit of TagItSmart, by providing secure authentication based on behavioural patterns. The tool provides a guarantee to the SMEs that the generated data are genuine and are not tampered as the users are continuously verified based on their behaviour. If SMEs do not trust that the authenticated users are genuine, they will not consider using such platform as they will not be confident about the collected behavioural data. In platforms that depend on the crowd, it is very important to establish trust among the stakeholders e.g. users, manufacturers and SMEs. This will lead to the establishment of trust between stakeholders and the platform as shown in the paradigm of the sharing economy [20]. These SMEs will face the aforementioned barriers in terms of lack of infrastructure, increased timescales and costs required for testing as they will not be able to use the TagItSmart platform.

Wider impact. BehavAuth will provide great economic benefits to those outside the project. The immediate and largest benefit is the cost reduction due to data leaks and password breaches. According to IBM every data leak in 2016 costs in average $4 millions for the company that suffered a cyber attack. This constitutes an enormous amount of money that will

be saved by deploying a secure and reliable authentication system that discards the need for the old-fashioned and vulnerable username/password system. In addition, organisations may reduce their costs as they will not need to spend resources towards training their personnel and developing software for enforcing different password policies. End users will save time, meaning improvement in terms of productivity as they will not need to perform time consuming and repetitive actions such find credentials, insert credentials, register, sign in, sign out. End users will be able to directly perform their work, as the system will have already authenticated them. On the EU economy side, start-ups such as Quadible will create new revenue streams with exponential growth and increase the government incomes through taxes and export opportunities. Also, BehavAuth will enhance the EU's position in the development of software products and especially authentication systems.

Social impacts. BehavAuth focuses on creating a user-friendly, secure and privacy preserving authentication tool. Authentication systems are often frustrating for end users as they need every time to create new username/password for each system, remember them or store them in a secure place. Often though, end users lose or forget their credentials leading to a stressful and time-consuming process, in order to successfully recover them. End-users will increase their trust towards on-line systems as they will know that their data are accessible only by themselves and their privacy is preserved. GCHQ released a new guide on how to shape a secure password, even requiring training for the personnel of an organisation on how to create a safe username and password combination. These guides could become obsolete as well as the training required for people to come up with a secure username/password. In addition, new job opportunities and research areas will emerge due to the growth and productivity improvement of the company. Government services could directly identify the users (depending on the sensitivity of the service) without the need of identification proof.

Environmental impact. The resources spent by the end users to remember and store the username and password for an online account will be obsolete, reducing the paper waste.

Regional Impacts. The regional impacts relate mainly to improvement of the growth and productivity of the startup. In the local scale, new job opportunities will be created in Guildford, employing a wide range of people; from students attending the local university, to experienced professionals. University of Surrey and SETSquared accelerator will benefit in terms of exposure and use case studies, as members of the team have received great assistance from them to establish the start-up. In a regional scale, Surrey county will receive great exposure due to the growth of the start-up and, in a national scale, new departments of the company will be established in other parts of the country. In long-term, the growth of the start-up will empower the EU position in the authentication market enabling export opportunities in global scale.

Section 2 - Co-creation activities

This section provides a detailed description of the dissemination actions taken in order to co-create the BehavAuth system by engaging stakeholders from the beginning of the project. The co-creation actions performed included the engagement of psychologists from University of London, University of Bath and University of Surrey as well as the initiation of engagement with an SME with psychologists called Behaviouralist.

2.1 Engaging psychologists

BehavAuth is a project that focuses on providing an authentication tool based on behavioural patterns of the users. This means that the authentication process is based on detecting the behavioural patterns of the users and based on them, to verify the identity of the device user. In order to correctly identify the behavioural cues required for the human behaviour recognition process, there is a need to engage psychologists. They will provide the know-how of understanding human behaviour and the knowledge about which behavioural cues provide the most significant information in order to verify a user.

As part of the BehavAuth stakeholder engagement plan was to engage psychologists from the beginning of the project. During this process, the BehavAuth team leveraged existing communication channels and also new ones, to contact various psychologists that could get engaged in the use case and requirement analysis process. Among the psychologists that were contacted were the team behind Behaviouralist [15], a consultancy that applies cutting edge behavioural science, economics and consumer feedback to solve behavioural challenges, as well as academics in the area of psychology from University of Surrey and Bath.

Among the various psychologists that we contacted as part of the system design and the dissemination of the project, Lisa Talia Moretti, a digital sociologist at University of Cardiff was engaged. Ms Moretti provided us various insights and information from the psychological aspect of the project. Some of the key points and behavioural cues that were mentioned are described below:

- **Average location or location hubs.** For most people, because of static locations of work/school/university and home (even the gym), they tend to frequent the same geographic area. Even for many consultants, who travel more than the average office worker, client work tends to be delivered around set project outcomes and therefore, even though their average location for work may change more than usual, there is a habit/pattern of behaviour that occurs during that timeframe. Indeed, consultants and the freelance community could be identified by their lack of average location stasis – a behavioural trait in itself.

- **Travel to our average location.** For many people, they have a tried and tested route to work and home. So not only is there a pattern that could emerge around an average location, but *how* people travel to those average locations is a pattern too. Does their average location include a train station? They are probably taking the train. Does it involve taking the back streets or main roads? The directions people take to travel to their average locations could become a key pattern to identifying them.

- **Speed and distance within the environment.** How we move around our environment is another behavioural trait worth exploring. For some it's by bicycle, for others by car, train or even, their two feet. This largely determines how fast we move and how many

steps on average, we take a day. Therefore, looking at how fast someone moves around their environment in addition to the relationship between speed and distance is important.

- **Relationship with our phones.** Studying how we hold, carry and store our phones could prove to be one of the most unique, small data points we have in identifying an individual. From hand to back pocket, or hand to handbag, in addition to whether you have a preference for taking photos landscape or portrait or indeed, whether you watch your videos landscape or portrait. In addition, there are small habitual movements that some people have developed when their phone is in their hands; spinning it around with two fingers, resting the long-edge on a flat surface while tipping it from side-to-side. In addition, the movement upwards towards an ear – indicating calls – versus, portrait being held still mid-air – indicating texting – would prove to be interesting small data points to capture; although this may not prove to be as useful because of people using headphones (whether tethered or untethered to the phone) to create a hands-free experience.

2.2 Engaging privacy experts

BehavAuth focuses on collecting sensor data from Internet of Things devices including smartphones in order to authenticate users to the TagItSmart platform based on behavioural patterns. The collected data that will allow the authentication of the users should be correlated with particular users, which will allow the differentiation among the users and further the identification of the users. Meaning that the data collected to identify the users are personal data. BehavAuth pays particular attention to the privacy and security of the users by recognising the existence of personal data in the authentication procedure. For that reason, from the beginning of the project, has defined some actions in order to preserve the privacy of the users. Among these actions are the engagement of privacy experts during the whole duration of the project who will provide feedback regarding the privacy aspects of the projects. Furthermore, an ethical review will be provided at the end of the project to evaluate the privacy issues that may arise during the project.

2.2.1 Digital catapult

As defined in the project plan and pointed out by the consortium of TagItSmart, BehavAuth engaged a privacy expert from Digital Catapult (UK), Dr Michele Nati. Dr Nati is a Lead Technologist for Personal Data and Trust with a great focus on privacy from the point of the end-users. QBE established a collaboration with Dr Nati, in order to receive feedback about the potential privacy issues that may arise during the project. The BehavAuth project was presented to the privacy expert including an overview of the initial tool design. Dr Nati provided feedback and considering the new European Commission data privacy protection scheme (GDPR), he helped us shape the initial tool design from the perspective of users' privacy. A few points that where highlighted from the privacy expert which need to be taken into consideration

- **Consent**. For each biometric or data that will be collected for the authentication of the user, there is a need to receive explicit consent from the user. The consent must be requested in clear and plain language. For example, in case the tool uses three biometrics, an explicit consent in plain language must be requested from the user for each one of the biometrics.

- **Breach notification**. In case of a breach, the end user needs to be informed at most in 72 hour from the breach.

- **Right to access**. Users are allowed to request confirmation if personal data is collected, where, and for what purpose. Furthermore, users could ask for the personal data collected, thus BehavAuth shall provide a copy of the personal data, free of charge, in an electronic format.

- **Right to be forgotten**. The entity or organisation that controls the personal data collected from the users, needs to provide the ability to the user to delete any collected personal data, to cease any dissemination of the data and potentially have third parties halt processing of the data.

- **Data portability.** User can ask from BehavAuth to receive the personal data concerning them and have the right to transmit that data to another company.

- **Privacy by design**. BehavAuth should collect and store only personal data that are necessary for the completion of the authentication process (data minimization), and refuse personal data access to people that are not immediately connected to the authentication process.

2.2.2 GDPR Seminar – Penningtons Manches LLP

Following to the interview with the privacy expert from Digital Catapult, as part of the dissemination activities, the BehavAuth project participated in the GPDR Seminar provided by the Pennington Manches LLP law firm [6].

Penningtons Manches LLP is a leading UK law firm which provides high quality legal advice tailored to both businesses and individuals. We address the specific objectives of each client through our flair and technical expertise and offer a personal service founded on a strong team ethic.

The main speaker of the seminar was Joanne Vengadesan. Joanne is a commercial lawyer, specialising in technology transactions and data protection. Her work encompasses structuring and negotiating contracts for complex technology projects, IT agreements, intellectual property and technology licensing, e-commerce and consumer law issues. Joanne has particular expertise in the electric vehicle sector, where she has been assisting a client on its contracts with key partners in relation to electric vehicle charge point infrastructure, as well as on consumer law issues. As an expert in data protection laws, she is advising numerous clients on data protection compliance in readiness for the forthcoming General Data Protection Regulation. She also has expertise in brand protection, and she and her team manage intellectual property portfolios on behalf of a wide range of clients.

After attending the GDPR seminar, some important lessons were learned regarding the applicability of the new regulation. Among them are the following:

- ***Biometric data***. This is a new category of personal data that are added to the GDPR. Biometric data are considered the data leveraged to perform technical processing of personal characteristics to confirm identification. For the use of biometric data there is a need to acquire explicit consent from the user.

- ***Internationality***. The new GDPR regulation is applied to the member states of the EU. However, in case a company is not based in one of the EU countries and trades in one of the EU then there is a need to comply with the GDPR regulation. For example, given

the foreseen Brexit where the UK with exit the EU, as BehavAuth focuses on trading also in the EU there will be a need by the BehavAuth to comply fully with the GDPR regulation.

- ***Breach management process***. According to the GDPR there is a requirement of mandatory notification of security breaches without undue delay and no later than 72 hours, if there is a risk to people's rights and freedoms. The data controller must document each breach, its effects and actions taken. Organisations should implement a data breach policy.
- ***Data Protection Officers***. Based on the GDPR data controllers and data processors must designate a DPO if the organisation is a public body or if core activities involve regular and systematic monitoring of personal data on large scale, or involve large volume processing of special categories of personal data. At this points, this is not applicable for BehavAuth.
- ***Accountability and on-going compliance***. Businesses need to demonstrate that they comply through a series of actions. Among them are internal policies and processes that comply with GDPR, implementation of policies and processes into the business's activities, use of data protection impact assessments, appointment of a DPO and signing up to a Code of Practice or certification scheme. There is a need to pay attention to the Privacy Impact Assessments.

2.3 Potential customers

As part of the system design based on the use cases and the requirement analysis is the engagement with potential early adopters of the BehavAuth. The early adopters of the platform constitute significant part of the design of the BehavAuth tool. This is because BehavAuth is creating a tool that considers stakeholders during the whole duration of the project, to receive feedback and to define the system based on the requirements of the stakeholders including the early adopters.

During the co-creational activities performed to create an authentication tool that fits the needs of the customers, BehavAuth team discussed with various potential adopters of the platform. Among them, were Pobuca [17] (a contact management platform) that assisted in the overall architecture of the system in order to allow the easy integration with various third-party platforms. In particular, they guided us on how to decouple the different components such as the user management from the core authentication mechanism. Other companies such as Illlumine [18] (a cloud and telecoms consultancy company) provided feedback about the cloud architecture required to provide a stable and robust authentication-as-a-service product. Public organisations that were also interested in the BehavAuth such as eID [16] and European Cyber Security Organisation [19], provided feedback regarding the need for scalability as well as the promotion of the product in the EU and how to better disseminate the work across EU and through the EC. Other SMEs such as TrueInvivo [20] (a radiation detection company) provided feedback regarding customer acquisition process.

The first early adopter of the BehavAuth tool is the TagItSmart platform, which will allow QBE to shape the use cases and the requirements based on the TagItSmart platform needs. Following, are the requirements extracted from the engagement with the early adopters of the platform:

- **Non-intrusive**. The use of personal data does not affect only the end-users but also the potential early adopters of the platform. This is because of the new EU regulation about personal data (GDPR [4]). Particular measures need to be taken by the adopters of the platform, to safeguard their organisations (including TagItSmart) in order to protect their users' privacy. TagItSmart consortium pointed out that it is important to utilise less intrusive personal data and to avoid methods such as face and voice recognition.

- **Low cost**. Pricing is always considerable when a third-party platform wants to adopt a new authentication solution. A reduced price in comparison to the solutions that are already in the market could intrigue third-party platforms to change to a more innovative authentication tool. The cost reduction could be also translated in terms of minimisation of security breaches, meaning that a more secure system could save money/reduce the costs for a third-party company without providing a 'cheaper' (in terms of pricing) solution.

- **Secure**. Security is imperative for authentication systems in order to convince third-party systems to discard any legacy authentication tools and to adopt innovative authentication tools such as BehavAuth. In order to achieve this, the BehavAuth tool needs to provide a more or equally secure solution as the state-of-the-art systems.

- **Compatible**. Compatibility is a very important requirement in the design of an authentication tool. State-of-the-art protocols and standards needs to be followed in order for the BehavAuth to be compatible with the majority of the third-party systems that are currently already in the market such as OAuth 2.0/OpenID and SAML.

- **Portability**. Depending on the third-party platform, it may already have a user management component. For that reason, the BehavAuth architecture needs to be portable in order to be able to operate both with platforms that do already have a user management component and with platforms that do not have a user management component and require from BehavAuth to provide that service.

- **Scalability**. The system needs to be scalable in order to be able to serve a large number of users independent of the workload and the number of requests. The BehavAuth tool will be implemented as an Authentication-as-a-Service on cloud infrastructure in order to enable the scalability of system.

2.4 End-users

End-users constitute a significant component of the project's stakeholders as they will be the actual users of the authentication mechanism. They will have direct access to the mobile app that will collect data from the smartphones' sensors and device usage data in order to infer the identity of the users. End-users will directly interact with the app. For that reason, it is imperative need to receive feedback from the end-users regarding the design of the system and in particular the mobile app. End-users need to provide feedback about the BehavAuth platform, in order to help us shape the tool based on the end-users' needs.

The end-users that were engaged in order to allow the co-creation of the BehavAuth tool together with the end-users, were diverse. This means that the people engaged were from different technical, educational and cultural backgrounds. As the product is focused on the majority of the people and not to a specific type of users, there was a need to engage people

with diverse background. Depending on the area of expertise the feedback from the users was different. Technical experts strived to retrieve more detailed information about the authentication process and “what is under the hood of this black box”. Less technical people focused their feedback on the privacy and security aspect of the project. Non technical people were mainly fascinated about the project and in some cases they expressed some concerns about the privacy and the intrusiveness of the system.

Following, some key points that were outlined by the end-users are described:

- **Training process**. There is a need to minimise the end-user involvement in the training process of the platform for a particular user. As mentioned the BehavAuth platform will learning the behavioural patterns of the user in order to authenticate them at the TagItSmart platform. Thus, the user involvement needs to be minimal in that process.

- **Privacy**. The data collected by the mobile app may be intrusive regarding the privacy of the user. BehavAuth needs to pay particular attention on the privacy aspect in order to safeguard the personal data of the end-users.

- **User-friendly**. The platform needs to be user-friendly and allow the user authenticate at the TagItSmart platform in an easy, fast and secure way.

- **Security**. The platform must provide a secure solution for the end-users and the TagItSmart platform, which minimises the vulnerabilities and improves the existing state-of-the-art systems. This requires a secure architecture of the overall system but also accurate machine-learning and artificial intelligence models that will allow the accurate and robust recognition of the behavioural patterns.

Section 3 - On-line dissemination activities

This section provides a detailed analysis of the actions taken from the BehavAuth in order to evaluate, secure and preserve the use of personal data in the platform.

3.1 Micro-website

As defined in the Description of Work, Quadible created a micro website as part of Quadible's main website www.quadible.co.uk The micro website was hosted at the company's hosting service under the domain www.quadible.co.uk/behavauth.The micro website was designed to provide the web-presence of the BehavAuth project and promote the authentication solution.

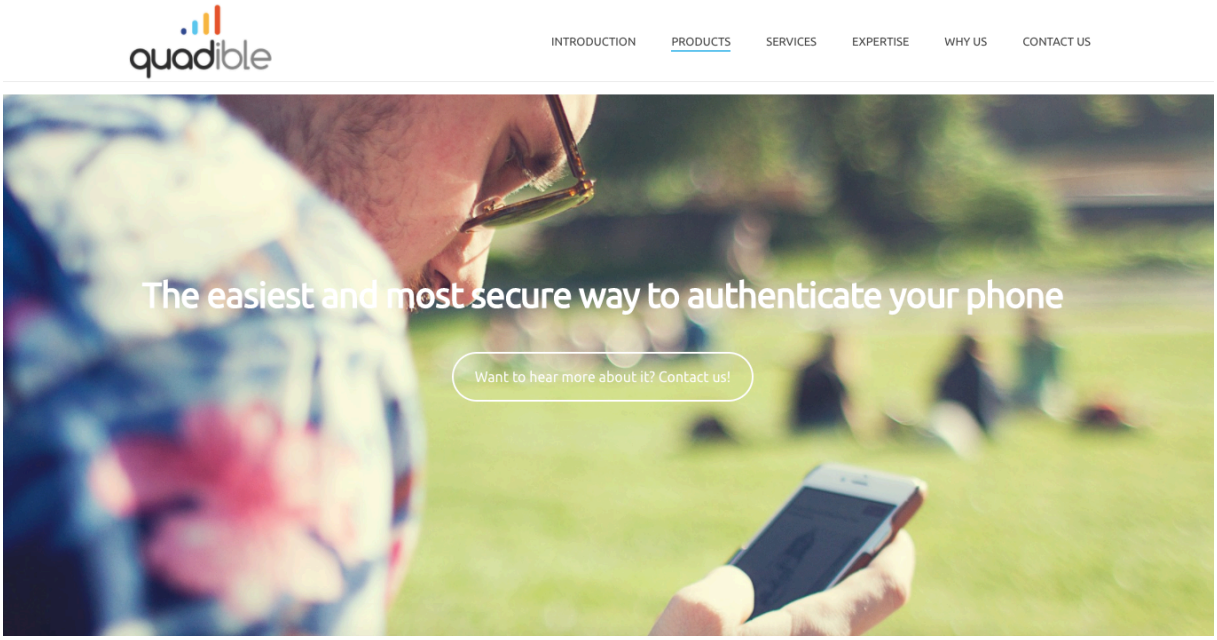

Figure 1. Screenshot of the BehavAuth micro website

The website was designed with a one-page parallax concept. This means that the content of the micro website is populated through one page, where the user scrolls down and can view the different information provided. Targeted taglines (See Figure 1) were included throughout the webpage in order to attract the readers and to enable them to engage and contact Quadible in order to receive more information.

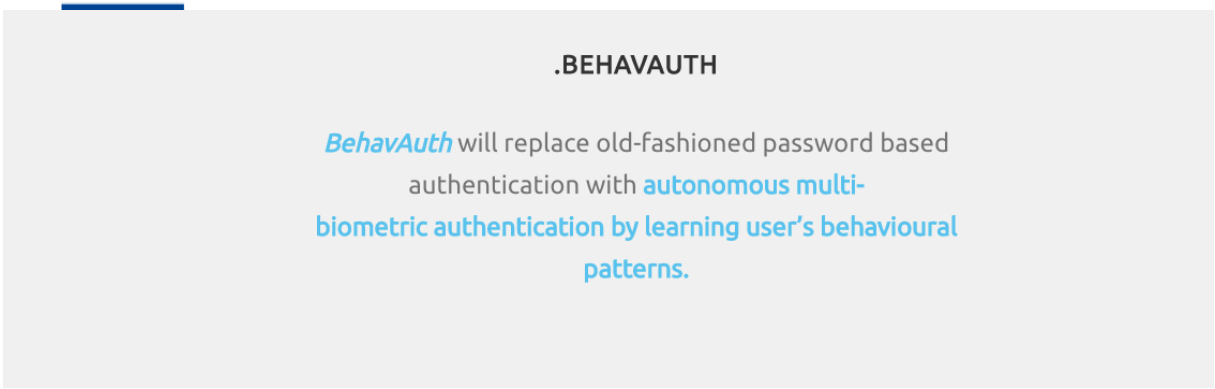

Figure 2. Screenshot of the overall description of the BehavAuth tool.

An overview of the BehavAuth project is provided (See Figure 2) initially to the viewers of the website in order for them to receive an overall understanding of the BehavAuth tool. This will trigger the interest of potential stakeholders that want to get engaged with the BehavAuth project as well as to trial the solution in their own context.

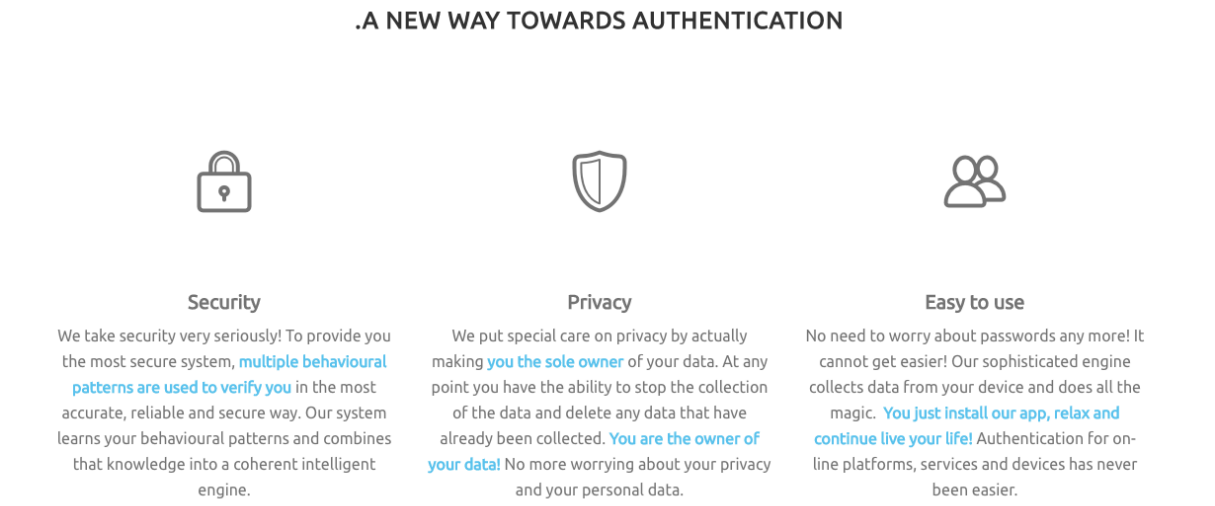

Figure 3. Screenshot of the key benefits of BehavAuth.

Following, the micro website provides an overview of the key benefits (See Figure 3) that the BehavAuth tool provides to the end-user. Among these key benefits are security, privacy and user-friendliness. A short description is also provided below every benefit, where the key benefit is analysed in more details as well as the way the BehavAuth achieves this. Each benefit includes 2-3 sentences that briefly describe how this is achieved by the BehavAuth, allowing the readers to fast and easily understand what are the benefits of adopting the BehavAuth solution.

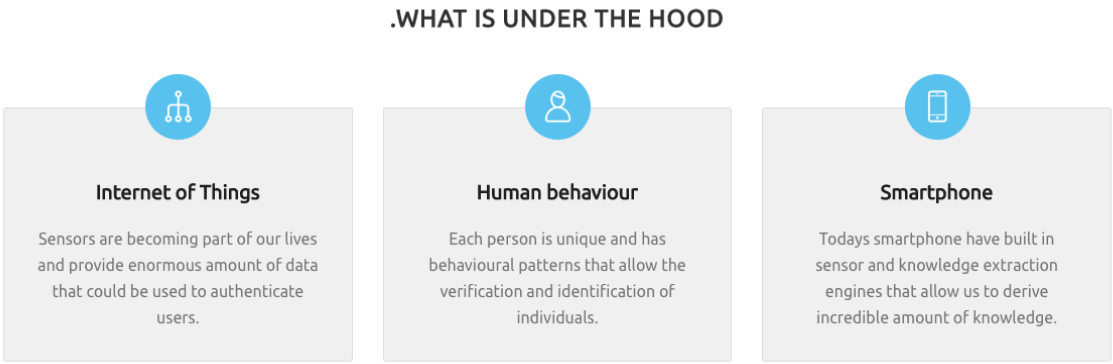

Figure 4. Screenshot of the key components of the BehavAuth.

The next section of the micro website provides an overall description of the key components of the BehavAuth solution. The key components are Internet of Things, human behaviour and commercial-off-the-shelf smartphones. The Internet of Things provides the ability to the BehavAuth solution, to collect data from multiple sensors and forward the data to the knowledge extraction engine in order to derive the authentication knowledge. The Internet of Things provides the ability to the BehavAuth to better understand the environment of the user and to retrieve contextual data to authenticate the user. The human behaviour constitutes the aspect that replaces the old-fashioned username/password in order to authenticate the user. The artificial intelligence and machine-learning models learn the behavioural patterns of the user and further provide the authentication result. Lastly, the smartphone is the key data collection device, it is a device that users carry with them constantly during their daily lives. In parallel, the computational power as well as the increased integrated sensors embedded on today's smartphones, make them ideal devices to collect behavioural data and further authenticate the users.

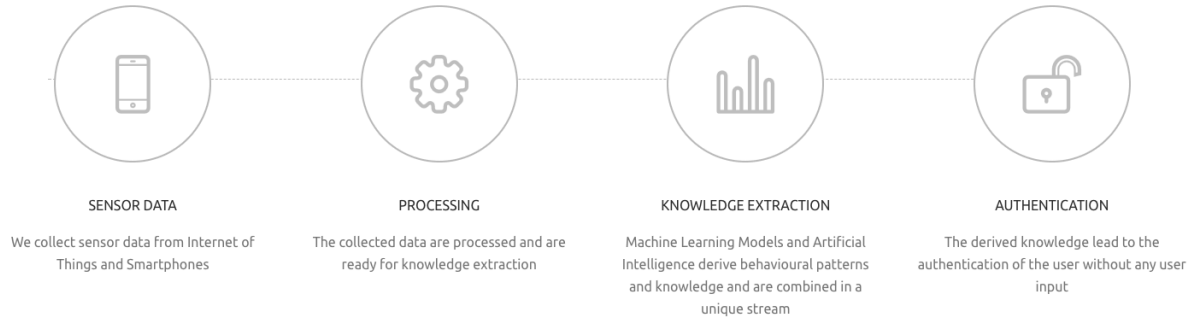

Figure 5. Screenshot of the authentication process.

The following section provides an overview of the process followed in order to authenticate the user. Figure 5 provides a schematic representation of the procedure followed to authenticate the user in a sequential manner. Initially, the data collection process is presented, followed by the processing and the knowledge extraction that lead to the authentication of the users.

Lastly, the micro website contains a contact form that enables the reader of the website to get in contact with Quadible in order to express interest about the BehavAuth solution. The contact details of the company are also displayed.

3.2 Social media

Social media are an important aspect of the on-line engagement activities. This is because the social media are engaging millions of people day and constitute a core component of the daily updates of these people. For that reason, BehavAuth leveraged these on-line communication channels in the area of social media in order to disseminate the work done in the project. Also, periodical press releases were performed in order to inform stakeholders about the progress of the project, potential meetings taking place as well as any news related to the TagItSmart project and the BehavAuth project.

The dissemination activities related to the social media were performed through Quadible's communication channels/accounts. This was done in order to leverage the audience that Quadible has already established through previous years. This was performed so there was no need to reinvent the wheel and continue the social media engagement from a certain level. Thus, the social media engagement was performed through Quadible's social media accounts on

- Facebook: https://www.facebook.com/quadible/
- Twitter: https://twitter.com/quadible
- LinkedIn: https://www.linkedin.com/company/quadible-ltd

3.3 Press release

In order to get more attraction to the BehavAuth project, Quadible leveraged existing communication channels such the memberships with SETsquared [8], M3GrowthHub [13] and Knowledge Transfer Network (KTN) [14]. In particular, Quadible is a member of the SETsquared incubator programme in the Surrey Technology Centre. Among many benefits included in the SETsquared incubator programme, is the ability to participate in the press release of SETsquared about important facts and updates about the company. Quadible performed a press release through the SETsquared network announcing the BehavAuth project and the support/collaboration with the TagItSmart EU project.

3.4 Scientific dissemination

The BehavAuth project has its roots in research and development. Thus following we are presenting the publications emerged from the BehavAuth project.

- A Prediction and Compensation Mechanism for Device Displacement Error, *"IEEE Transactions on Human-Machine Systems'* (submitted)
- Modelling Social Interaction Detection with Smartphones in Real-world, *"IEEE Transactions on Computational Social Systems*" (submitted)

Section 4 - Events – MeetUps – Conferences

This section provides a detailed description of the events, meetups and conferences that the BehavAuth team attended in order to promote both BehavAuth and TagItSmart projects.

4.1 Open calls kick-off meeting (Vaasa, Finland)

The first event that the BehavAuth team attended was the kick-off meeting of all the TagItSmart Open Call winners in Vaasa, Finland. This constituted a great event for the TagItSmart consortium to get together with the Open Call winner and co-create the TagItSmart platform as well as the tools to be built.
At the being of the meeting each TagItSmart member and Open Call winner introduced themselves. An initial introduction was performed by the TagItSmart consortium. Then each of the Open Call winner had around one hour to present the work to be done during the 6-month period. During the presentations, the TagItSmart consortium provided constructive feedback to each of the Open Call winner.

A BehavAuth project member presented also the work to be done in the BehavAuth project. The feedback from the TagItSmart consortium and the rest of the Open Call winners was related to the below main points:

- **Privacy issues**. TagItSmart consortium members outlined the importance of privacy in such a project. BehavAuth leverages personal sensor data to extract behavioural patterns of the users in order to authenticate them to different services. It is clear that the BehavAuth project uses personal data in order to identify the behavioural patterns of the user and further if they are the owners of the device or not. Given the discussion with the TagItSmart consortium it is imperative to perform an ethical review regarding the personal data collected by the BehavAuth tool, considering also the upcoming new EU regulation for handling personal data.
- **Exploitation plans**. TagItSmart consortium pointed out the importance of focusing on one application area. A common mistake of start-ups is the fact that they believe that their solution constitutes the silver bullet. For that reason, the TagItSmart consortium pointed out that it should be better to focus on one application area or market. This will enable the understanding of any potential shortcomings of the service as well as any significant barriers in adopting the behavioural-based authentication service. After having established a certain range of customers in the initial market, the BehavAuth could focus on expanding and scaling the solution to other markets also.
- **Privacy in the market**. TagItSmart consortium described also the potential privacy problems that could occur in different applications areas. Depending on the market that the BehavAuth will focus on, then particular care should be taken in order to identify the market that is keen on adopting innovative technologies and that has already exploited some kind of personal data. This will enable the adoption of a new technology in the authentication area that takes into the users' personal data.
- **Importance of behaviour in authentication**. TagItSmart consortium expressed their interest in understanding which behavioural cues and behavioural patterns constitute the most informative in the authentication process. Behavioural cues and patterns have different significance in the authentication process. For example, state-of-the-art techniques have successfully leveraged the fingerprint, iris recognition and face recognition for authentication. This indicates that these behavioural cues have greater significance than the location of the user that cannot be used as a standalone behavioural cue to identify a person for example.

4.2 ICT Proposers Day 2017 (Budapest, Hungary)

The ICT Proposers Day [12] constitutes a conference that takes place once per year at different countries in Europe. ICT Proposers' Day 2017 took place on 9 and 10 November 2017 in Budapest, Hungary. This networking event centred on European ICT Research & Innovation with a special focus on the Horizon 2020 Work Programme for 2018-20. An Opening Ceremony and Social Event was organised by the Hungarian Ministry of National Development and took place on 8 November. Initially this event provides information to attendees about the different EU calls for funding by the European Commission. In parallel, it provides great networking opportunities for the attendees.

BehavAuth attended the ICT Proposers day to find additional funding opportunities for the project and to promote the project to potential adopters or collaborators. This conference constituted the most significant event to attend by the BehavAuth project given its financial benefit as well as the exploitation and dissemination opportunities that this event provided.

The additional funding opportunities would constitute vital for the continuation of the project and would speed up further the development and also the scaling of the product to different markets. The funding received from the TagItSmart project was a great kick-off investment that allowed Quadible to create and launch an initial product. However, there is a need to reach the breakthrough point where the income of the BehavAuth product will overcome the expenses required for its maintenance. In addition, to maintain, develop further and scale a Software-as-a-Service product such as BehavAuth, there is a need to attract further investment. This will allow BehavAuth to reach faster its 5-year targets and to overcome the competition.

In addition, the ICT Proposers Day provided various ways to network with other potential collaborators. Among these many opportunities, a great event organisation allowed face-to-face brokerage, meaning attendees could meet for 10 minutes face-to-face on a desk and discuss about their needs and services. BehavAuth attendee had more than 10 meetings with potential stakeholders and collaborators that could constitute early adopters of the platform. Among them were an EU Project Manager of Athens International Airport, an EU Project Manager for Athens Municipality consultancy company and an EU programme manager for Aptoid (android app store +10M users).

The most significant outcome for this event was the initiation of engagement with the EU programme eID [16]. This is an EU funding programme that focuses on helping public and private Service Providers extend the use of their online services to citizens from other European countries. Among the many components of this programme is the development of a uniform identity system accord Europe, where even though each country uses a different citizen identification system, through the eID all these different identification tools are interconnected and citizens could be identified in different countries using their own identity mean.

BehavAuth attendee got in touch with the EU representatives from the eID system. They expressed their interest towards the BehavAuth solution. After receiving permission from the TagItSmart coordinator, the BehavAuth initiated engagement with the EU representatives in order to further disseminate the project. Each of the EU country-members has its own representative for the eID system. BehavAuth will initiate the engagement with each of the eID representatives in the different EU countries in order to further disseminate the work and promote the adoption of the BehavAuth tool as a universal authentication mean. Also, an initial

contact has been made with the EU Login project [21], which is the European Commission own authentication platform.

4.3 Santander Breakthrough Event (Guildford, UK)

Santander, one of the biggest banks in the UK, organise around the UK an event called Santander Breakthrough Event [11]. According to Santander, this event is focused on "helping ambitious businesses to succeed". Santander strives to build long-lasting relationships with SMEs and also focuses on understanding the needs of the customers. These events are focused on helping SMEs to break through and continue to grow.

Quadible was invited through the SETsquared incubator in the Surrey Technology Centre in Guildford. Attending this event constituted a great experience given the great networking opportunities as well as the interesting speakers that allowed Quadible to receive feedback on the BehavAuth project and how to further develop it and scale it.

Other SMEs that attended the event provided great feedback about the BehavAuth project. A common ground that was pointed out by all the attendees of the event was the great innovation and potential that a behavioural based authentication could offer. This indicates the great potential that the BehavAuth could achieve.

Another impact of the project was that Quadible become aware of a scheme provided by Santander in order to partially fund an intern for 10 weeks. In this way, Quadible will be able to engage an intern that will assist in the development of additional functionalities of the BehavAuth project and provide additional help in the continuation of the project.

4.4 GDPR Seminar (Basingstoke, UK)

The EU General Data Protection Regulation (GDPR) is set to replace the current Data Protection Act in May 2018. This will be a major shake-up of the law in this area, and in almost all cases will require business planning and changes to legal processes and documentation.

In January 2018, Penningtons Manches [6], a law firm with expertise in personal data, hosted a seminar for SETsquared members on the key implications of the GDPR [7]. As Quadible is a member of SETsquared incubator in Guildford, BehavAuth project attended this seminar in order to understand the key obligations and changes that are applied with the new personal data regulation and how would this affect the BehavAuth tool.

The main subject of the seminar was "what does the GPDR mean for businesses". This included various topics related to mainly online businesses and how to handle the new regulation that will be applied in May 2018. Among the topics covered by the seminar were key obligations and changes including enhanced rights of the data subjects (i.e. people), consent and legitimate interest, privacy by design, transferring data overseas, accountability principle as well as sanctions and enforcement. In addition, during the seminar there was a discussion about the GDPR readiness and how to prepare for the new regime including things like immediate steps, data mappings and gap analysis, ongoing considerations, handling data breaches and data protection issues in contracts.

The key aspects that were extracted from the seminar are outlined in Section 2.2.2. For further details, the reader is directed to the particular section.

4.5 SETSquared Club meeting (Guildford, UK)

Quadible is part of the SETsquared [8] network as a company and also hosts the offices of the company at the SETsquared incubator in Guildford, UK. SETsquared is a collaboration between the universities of Bath, Bristol, Exeter, Southampton and Surrey which partners in enterprise activities and collectively supports the growth and success of new business opportunities through spin-outs, licensing and incubation.

Surrey SETsquared is organising regular networking sessions [9] as a way to introduce new members to the SETsquared network and provide a face-to-face communication channel among the members. The main purpose of these meetings is to introduce and connect new members to current members that have not been yet introduced. Also, members are provided the ability to present any news and constitute a dissemination channel for each of the members. Among the invited meeting participants are also the SETsquared mentors and also a selection of companies from the SETsquared Affiliate Network.

During the meeting, Quadible member introduced the company as well as the BehavAuth and TagItSmart projects. Members showed great enthusiasm for the behavioural-based authentication tool. Members indicated the innovation in such a tool. Two members expressed their concern about the privacy issues and about the accuracy of the authentication process. In overall, members provided great feedback about the authentication tool.

4.6 MeetUp Internet of Things (Guildford, UK)

The final event that the BehavAuth project team attended throughout the duration of the project, was the MeetUp Internet of Things in Guildford [10]. The MeetUp was focused on guiding SMEs on how to enter the GDPR era. The MeetUp was organised by a privacy expert Dr Michele Nati from Digital Catapult [5]. The theme of the MeetUp was focused on businesses that collect and process personal and Internet of Things data from their customers and how the GDPR will affect these businesses.

The EU GDPR workshop at the MeetUp was focused mainly on the transparency introduced by the new regulation and also on the users consent and how to apply this in different Internet of Things businesses. People from different backgrounds attended the MeetUp enabling a holistic discussion among the participants.

The MeetUp provided great benefit in terms of the knowledge about the GDPR regulation and how BehavAuth can become compliant. In addition, various networking opportunities arose during the MeetUp, where the BehavAuth team had the ability to introduce the BehavAuth project and the TagItSmart project and discuss about the vision of the projects.

Section 5 - Conclusion

This deliverable described the impact and dissemination activities that were introduced throughout the duration of the BehavAuth project. The dissemination activities had their main focus towards promoting the adoption of the BehavAuth and TagItSmart platforms, and engaged from the beginning of the project all the involved stakeholders.

This document started by describing an overview of the impact and dissemination activities achieved during the BehavAuth project and further after the end of the project. Initially an overview of the dissemination activities performed was outlined defining the key points of the dissemination activities. Following, the impact achieved through the BehavAuth project and the foreseen impact after the end of the project as Quadible will ensure its continuation. The impact was categorized in terms of the benefit towards SMEs and the TagItSmart platform, as well as the wider, social, environmental and regional impact.

Next, the co-creational activities conducted in the BehavAuth project are analysed and detailed with respect to each stakeholder category. BehavAuth project engaged various stakeholders throughout the whole duration of the project. Among the stakeholders were psychologists to enable the team to conclude on the grammar of the behavioural cues in order to authenticate users. Then, privacy experts were engaged in order to ensure the correct handling of personal data with respect to users' privacy. Many end-users were engaged in the design and development process to understand the needs of the end-users and provide a user-friendly and user-centric design. Lastly, potential customers were engaged to understand the needs of various organisations that require an external authentication service for their users, and to design a system that can be secure and easy to integrate with third-party companies.

Following, the action taken to disseminate the BehavAuth and TagItSmart projects on-line presented. The action taken to disseminate the included the design and development of the web presence of BehavAuth through a micro website. The micro website is co-hosted at Quadible's website. It is a one-page website including information about the functionality provided and the actual service. Next, Quadible's existing social media on Facebook, LinkedIn and Twitter were leveraged to promote both BehavAuth and TagItSmart projects and promote the engagement of the stakeholders. Also, existing community networks that Quadible is member, were used to perform press releases about the BehavAuth and TagItSmart projects. Lastly, the scientific dissemination activities and publications that were achieved during the BehavAuth project were presented.

Finally, a discussion about the events, conferences and meetups that the BehavAuth team attended in order to disseminate the work in the project, was provided. Each of the events attended were discussed and analysed, while providing a description of the benefit provided to the BehavAuth and TagItSmart projects.

This document constitutes a report about the impact and dissemination activities performed throughout the BehavAuth project in order to promote and disseminate the work done in both the BehavAuth and TagItSmart project, while promoting the adoption of both platforms.

Section 6 - References

1. EU GDPR - https://www.eugdpr.org/key-changes.html
2. BehavAuth D1.1 Initial design based on the use case and requirement analysis
3. TagItSmart EU project – www.tagitsmart.eu
4. General Data Protection Regulation - http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
5. Digital Catapult - https://digital.catapult.org.uk/
6. Pennington Manches - https://www.penningtons.co.uk/
7. GDPR Seminar in Basingstoke - http://www.surreyincubation.co.uk/events/gdpr-seminar-in-basingstoke
8. SETsquared Partnership - http://www.setsquared.co.uk/
9. SETsquared Wednesday club meeting - http://www.setsquared.co.uk/event/setsquared-surrey-wednesday-club-event-members-only-0
10. MeetUp Internet of Things Guildford - https://www.meetup.com/Internet-of-Things-Guildford/events/246235093/
11. Santander Breakthrough Event - https://www.santandercb.co.uk/breakthrough
12. ICT Proposers Day 2017 - https://ec.europa.eu/digital-single-market/en/events/ict-proposers-day-2017
13. M3GrowthHub - https://www.enterprisem3growthhub.co.uk/
14. Knowledge Transfer Network - https://ktn-uk.co.uk/
15. The Behaviouralist - http://www.thebehaviouralist.com/
16. eID - https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eID
17. Pobuca - https://pobu.ca/
18. Illumine - https://illumine.gr/
19. European Cyber Security Organisation – http://www.ecs-org.eu/
20. TrueInvivo - http://www.trueinvivo.co.uk/
21. EU Login - http://ec.europa.eu/research/participants/docs/h2020-funding-guide/user-account-and-roles/ecas-login_en.htm