



# HAT Foundation Group

---

## **A Response to the Creation of Passport for Life from The Careers and Enterprise Company**

*Dr Susan Wakenshaw, Professor Irene Ng  
University of Warwick  
Dr Xiao Ma, Jonathan Holtby, Anna DeWolf  
HAT Community Foundation*

*Released 28 April 2017*

## **Who we are**

The Hub of All Things (HAT) Foundation Group is a consortium of organizations that partners with, and/or use the HAT personal data exchange platform by integrating HAT personal data microservice accounts (PDMA) as user accounts on their applications/services. The consortium is managed by the non-profit, members owned HAT Community Foundation, based out of Cambridge and London. The group run events for technology founders, developers, and researchers across the UK, Asia, and North America to support the growth and innovation of the next generation of Internet services on the open sourced HAT Technology.

Websites:

<https://hubofallthings.com>

<https://hatcommunity.org>

## **About the HAT**

The Hub of All Things (HAT) is a personal data exchange ecosystem designed through multiple RCUK funded projects totaling more than £3m and involving 6 universities and 20 partner organizations. In 2016, the operationalization and implementation of the ecosystem was passed to the HAT Community Foundation and the HAT Data Exchange. The HAT technology lets everybody – users, organizations and developers, exchange and trade personal data without sacrificing ownership. Its network gives citizens a private ‘microserver’ data account that helps them control and process their personal information easily, much like the way they manage a smartphone. The individual legally owns their HATs and the data contained inside, allowing them to be the data controller. The HAT technology infrastructure facilitates the secure transaction of this data. Individuals can exchange data between themselves in private HAT2HAT dialogues, or with external entities in exchange for services. The HAT is fully open sourced and organizations can provision private data accounts to their customers under their own brand, powered by the HAT.

# A Response to the Creation of Passport for Life (Pfl) from The Careers and Enterprise Company<sup>1</sup>

## 1. Benefits of Passport for Life

Passport for Life (Pfl) would bring about various benefits addressing the gap between education and workplace. Economically, Pfl has the potential to reduce the unemployment rate among young people by filling vacant jobs with young people with appropriate qualifications and skills. This could be achieved through: (1) enabling or guiding young people to identify how to improve their skills, and in what areas. This would enable young people to develop relevant skills and therefore would reduce the gap between the skills required by employers and the skills possessed by young people. (2) Allowing organisations to offer young people meaningful opportunities for developing and strengthening their skills for their career development, either through encounters with the world of work, or extra-curricular activities. (3) Allowing organisations to offer the right employment to young people with the right skills and experiences.

Socially, Pfl would enable the development of a community working with the shared purpose of reducing the gap between education and the workplace. This could be achieved through a platform-driven business ecosystem, and through the enhancement of service innovations within that ecosystem through the integration of the resources of multiple organisations, individuals and young people. This would allow organisations to reach out to young people from all walks of life, including less advantaged young people who may not have benefitted from careers advice services or resources previously. This could result in young people from lower income families, who are traditionally hit harder by the skills gap, developing the right skills to find advantageous jobs, ultimately improving social mobility and countering inequality.

However, in order to harness the benefits of Pfl, we suggest that the following challenges need to be addressed. We discuss the challenges by looking at the three components of the Pfl platform.

## 2. Challenges for Passport for Life

### *A database/distributed data structure*

Digital records of achievement are used in schools, colleges and universities across the country. Passport for life would pose '*an integrated verified record of a young person's achievements which draws together data from all partner organisations*'. Various types and forms of information, such as courses, grades, extra curricular activities, work experience and employment could be included in such an integrated record.

Challenges:

---

<sup>1</sup> <http://www.careersandenterprise.co.uk/news/can-you-help-us-create-passport-life>

- (1) Interoperability: Dealing with data of different forms and types, and drawing intelligence from that data for different purposes.
- (2) Integration and ownership: Creating an integrated verified record requires all the data (distributed in different database) to be pulled into one database. The question is a) whether the database would be centralised or distributed; b) who would own the database. The answers to these questions would have significant implications for the privacy and security of the personal data held therein.

#### *A data access layer (APIs)*

Information could be added by multiple entities, including students, schools and external groups such as the Duke of Edinburgh Award or National Citizen Service, either manually or via an API (Challenge 3, see below). Information would require verification by organisations (e.g. government, employers or organisations providing relevant activities) (Challenge 4, see below). A platform would also need to handle identity matching across those multiple sources (Challenge 4). Furthermore, the platform would need to provide a mechanism for users to consent to their information being used in the system, as well as ensuring that the information is used in line with that content within the system (Challenges 5 and 6, see below).

#### Challenges:

- (3) Access Control: This would cause a significant privacy concern for personal data, in terms of its collection, storage, access, the purpose of its usage/analysis, and its dissemination. If the information must be added by multiple entities, the right to access the information would be problematic. This could lead to both confidentiality and security issues.
- (4) Source Verification: Information in any given record would need to be verifiable by various organisations. It would also require those organisations to be accountable for that information. The management of such a system, with several points of verification dependency could lead to security issues.
- (5) Meaningful Consent: Consent has to be informed and also meaningful. Meaningful consent entails control and understanding of any implications surrounding the results of that consent. Young people could be vulnerable in terms of their skill and capability to make decisions on how their data could be used, for what purposes, and their implications. The challenge is in creating a mechanism to enable young people a) to understand what they are consenting to; b) to reduce the overwhelming number of precise data requests to which they may be required to consent; c) to make the consent mechanism more effective and efficient.
- (6) Trust Anchoring: Establishing trust between young people and the system, and between young people and the organisations proposing to use their data based on the agreed purpose, and assuring actors in the system that the use of data *is* for the agreed purposes.

#### *A possible basic portal application*

The users for the platform include young people, employers, training and volunteering organisations, schools, parents and other organisations with responsibility for a young

person's future. However, these users have different purposes, needs and objectives. How to create values for these users is crucial for the adoption and use of the platform (Challenge 6).

Organisations would present information about young people's achievements, activities and skills. Analysis would then be provided in terms of generic recommendations regarding potential careers and/or opportunities to develop skills (Challenge 7, see below).

'Presentation/notification of targeted suggestions of specific opportunities to develop skills, engage with employers, find work experience or apply for employment or training' (Challenge 7 and 8, see below).

Organisations could submit information as part of an application for employment, training or extra-curricular activity. Through the principle of 'privacy by design', information could be used without identifiers and consent managed through notifications and preferences regarding the extent of information submitted as part of an application' (Challenge 3).

Challenges:

(7) Personalised Service: Defining how these generic recommendations could be meaningful and valuable to the young person. The young person needs to initiate and be involved in the process of analysis and the generation of the recommendations; recommendations coming entirely from third parties without any engagement from the individual would not be as effective as active analysis and involvement from the individual.

(8) New Service Discovery: Identifying and defining gaps between skills and experiences and the generic and specific jobs, training or apprenticeships desirable for young people.

With the identification of the challenges to address, we propose the following potential solutions.

### **3. Proposed potential solutions**

#### *PfL Ecosystem*

We suggest that an ecosystem could be developed for the PfL platform. This should have trust anchoring from a third party, ideally a not-for-profit organisation. This organisation would be responsible for the onboarding of data sources, providers and individuals, and would endorse a collective monitoring and rating mechanism designed to support and regulate the community. The notion of a PfL ecosystem is based on the concept of the service ecosystem (Vargo and Lusch, 2016). Vargo and Lusch (2016) proposed the notion of a service ecosystem, which is a self-adjusting system of resource integrating actors connected by shared institutional arrangements and mutual value creation. All the actors co-create value in their contexts through resource integration, service exchange and provision, coordinated by the institutions and institutional arrangements. All the actors interact, exchange and integrate their competences for value co-creation and thus result in the overall well being of the system. The resource integration for value co-creation could be coordinated by keystones represented

either by a few organisations and with a platform, and/or by some shared agenda, rules and agreement. This notion could address Challenge 6 in terms of value co-creation and enhancement young people's engagement with the platform. This would also fulfil the social value of PFL.

#### *Personal data platform (Challenge 1; Challenge 2)*

A young person's information on achievement and experiences are in various type formats (courses, grades, extra curricular activities, work experience, employment), and are situated in the databases of multiple organisations. Passport for Life would be 'an integrated verified record of a young person's achievements which draws together data from all partner organisations'.

Even if data access and acquisition could be standardised, to use it requires a level of transformation capability that individuals often do not have. The data would need to be re-categorised and contextualised which could address Challenge 1. We propose that young people could control the collection, storage and analysis of their data, and give consent to the analysis of their data by various kinds of service. Importantly, the digital record needs to be owned by the individual, which could overcome Challenge 2.

HAT ([hubofallthings.com](http://hubofallthings.com)) technology and ecosystem has addressed the challenge through the transformation of personal metadata from unrelated 'verticals' into a 'matrix' format. This requires, firstly, the separation of contextual metadata (parameters that change in context – for example, feeling hot or hungry) from acontextual metadata (parameters that do not change in context – eye colour, a shoe's brand). The value of services are realised in context, hence, it is within the context of 'horizontal' lived lives that offerings create value with individuals. This implies a need to separate what is acontextual with what is contextual so that the 'horizontal' can be derived. The HAT takes the parameters of a value proposition as acontextual and the parameters of value creation as contextual. Metadata of 'in-use' and 'in-context' must be separated from 'static' metadata on objects and services. HAT is a person-oriented personal data platform, owned by the individuals. On this platform, individuals would be able to contain, flatten, bundle and exchange all types of personal data. This in turn allows personal data to be contextualised and bundled, or integrated with other data sets in a way that is privacy-preserving and controlled by the user, so that smart individuals can benefit from crowd-sourced information and better, informed decision making. Equally, the HAT enables commercial organisations to be equipped with the same technology to receive and process personal data from individuals and potentially to share their own proprietary information with the individual, for better personalisation of their offerings.

#### *Private Data Microserver Account (PDMA) (Challenges 2, 3 and 4)*

For the integrated digital record, the privacy concerns associated with the 'control of personal data' and the security of personal data are the biggest challenges. In fact, we propose that these challenges could be addressed through the proliferation of private, standalone databases for personal data that can be owned, solely controlled, and used by individuals. These privately owned databases have the potential to make individuals data controllers and processors. This can be accomplished through the use of containers, which encase various discrete components of application logic and require only minimal resources to do their job.

Unlike virtual machines, containers do not need an operating system. Instead, they call for operating system resources via an Application Programming Interface (API). Containerising databases in this way can isolate them at the (micro) server level.

The content within them can be encrypted and backed up regularly, and traditional direct database access can be replaced by server-level API calls. This isolation creates an added extra layer of security, localising the impact of any breach and mitigating the risk) of sys-admin granted unauthorised access. Widely adopted, the number of personal user accounts that sit within apps and services worldwide could be systemically reduced, eliminating pervasive cyber security vulnerability and greatly reducing the incentives for cyber attack. A penetration into one secure database container yields the perpetrator of that attack exactly one database, where in the current system a similar risk would yield up to billions of records of personal data instead. This would address the confidentiality concerns and security challenge laid out in Challenge 2. For more on PDMA's, [please see the white paper on digital dependency](https://www.hatdex.org/digital-dependency/) (<https://www.hatdex.org/digital-dependency/>).

Containing one individual's data within an entire database allows the individual themselves to be a data controller and to some extent a data processor, operationalising the bundle of rights to which they are due. This could address the privacy concerns about the individual control of personal data – Challenge 3.

Verification of the identity from multiple resources would require the young person to create many Internet accounts. Managing so many accounts is inconvenient in the extreme to the individual, and a cyber security risk to society. At the same time, it is impossible to enforce personal data regulation. PDMA's could be a potential solution for the verification of information and identity management in a secure way, addressing Challenge 4.

#### *Digital Butler and meaningful consent, Challenge 5*

One challenge for the PFL platform is consent: how to make the data requests they are allowing understandable to the young people using the platform, and enabling them to understand the implications of their consent and control the use of their data. Other questions raised include who could give consent on behalf of the young people who are vulnerable in certain contexts; and how to avoid overloading the consent requests and use AI to learn users' preferences and to make automated consents. For example, the notion of digital butler has been proposed by researchers at Southampton University to address these issues.

#### *Distributed Ledger Technology (DLT), Challenge 6*

Technically, we would propose to use Distributed Ledger Technology (DLT) designed to achieve trustworthiness, availability, security, and the desired level of cost adjustment. We would employ the target architecture. The target architecture is built on the possibility to create a DLT, governed by a non-profit regulatory body, in which the choice and operation of cryptographic puzzles, which drive the creation of new blocks of data from other verified sources, are controlled and owned by one or more organisations, as demonstrated by Lundbaek et. al. (2016). This architecture will respond to the relatively new emphasis on networks and their members in the business ecosystem (Iansiti and Levien 2004) and the

recent shift from individual rationality to cooperation and sharing economy (Vargo and Lusch 2016).

*Collaborative platform for competence management, (Challenges 7 and 8)*

Technically, the questions of how to identify the gaps between required and possessed skills and experiences, and how to bridge these gaps by providing opportunities for training and experiences are challenging. Moreover, how to the best match between what is offered by organisations and what young people really want is very challenging.

We propose that Pfl could become a platform for collaborative competence/skill management. For example, WMCCM (<http://www.wmccm.co.uk/WMCCM/DesktopDefault.aspx>) is a platform for competence management, which could optimally match the competences needed for new product or service and the competence possessed by using network analysis and identify and bridge the gap between competences. We propose that by creating this type of platform, all skills required for careers and jobs could be categorised; training and education programmes could be categorised in terms of the skills or experiences to be developed; furthermore, young people's achievement could be categorised against these skills. Then the young people could identify their own gaps in terms of their skills and the skills required to identify the training and education programmes to reduce these gaps. For organisations, the opportunity arises to design training and education programmes and identify the young people who need this training based on the skill gap analysis. The platform would also help organisations identify the best candidates for their jobs, and the platform would apply these jobs on behalf of the young people. We can envisage that this competence management platform would generate many new services and would create value for all the actors in the ecosystem. This could enable the Pfl to achieve its economic and social goals.

The above response is a response based on mapping the challenges described by the call issued by the Careers and Enterprise UK (<http://www.careersandenterprise.co.uk/news/can-you-help-us-create-passport-life>). In sum, we see the HAT platform technology as ideally suited to meet the challenges through PDMA provisioning and exchange of data between parties. However, the HAT technology is adopted by several HAT Service Providers and they may differ in the way they propose to implement the capability (if invited to propose). The HAT Foundation Group does not endorse any particular provision but seek only to provide an evidence-based response and advice to CEC challenges laid out in the call.

For more information, please contact the HAT Community Manager, Jonathan Holtby at [jonathan.holtby@hatdex.org](mailto:jonathan.holtby@hatdex.org)

The authors acknowledge the contribution of the following members of the HAT Foundation Group in crafting this response:

Professor Glenn Parry, University of West England  
Professor Jon Crowcroft, University of Cambridge  
Professor Roger Maull, University of Surrey

**References:**



- Iansiti, M., and Levien, R. 2004. *The Keystone Advantage: What the New Dynamics of Business Ecosystems Mean for Strategy, Innovation and Sustainability*. Harvard (MA): Harvard University Press.
- Leif-Nissen Lundbaek, Andrea Callia D'Iddio, and Michael Huth. Optimizing Governed Blockchains for Financial Process Authentications. 1 December 2016. arXiv.org > cs > arXiv:1612.00407
- Vargo, S.L. and Lusch, R.F., 2016. Institutions and axioms: an extension and update of service-dominant logic. *Journal of the Academy of Marketing Science*, 44(1), pp.5-23.