Certification for HAT Platforms and Services
HAT Code of Practice

HAT Community Foundation
The scheme authority of the HAT Foundation

Working to allow everyone to trade their data with
privacy, confidentiality, security and trust

www.hubofallthings.com

HAT Community Foundation, Registered in England No 9933330
Registered address: The Cottages, 8 Comberton Road, Barton, Cambridge, CB23 7BA

Contents

Purpose and Scope

This document outlines the process for the certification of HAT Platform and Service providers for admission to the HAT Ecosystem. Anyone (any natural person or corporate body) must be certified in accordance with this process before they can contribute assets (including but not limited to platforms, services, applications and other products) to the HAT Ecosystem.

This process and the Hub-of-All-Things™ logo is owned by HAT Community Foundation (HCF) which is the HAT scheme authority working on behalf of all HAT users to ensure that the HAT Ecosystem is regulated for the private and secure exchange of personal data. Certification for participation in the HAT Ecosystem requires agreement to and compliance with the requirements detailed in Appendix A and B, the certification check-list, and Appendix C. Anyone seeking certification will submit answers and supporting evidence to HCF in confidence**,** who may then audit responses before issuing a Certificate of Compliance (Certificate) with the HAT Code of Practice and Trust Framework.

As well as allowing admission to the HAT Ecosystem, the Certificate grants a licence to the holder to use the Hub-of-All-Things™ logo and associated certification marks.

The HAT Community Foundation has licenced HAT Data Exchange Ltd (HATDeX) to act as the HAT scheme operator. As such, HATDeX may act as HCF's agent for the Certification of HAPs and HSPs and is licenced to issue SSL Certificates and GUIDs as appropriate to anyone holding a HAT Certificate of Compliance.

NOTE: HATDeX is the HAT scheme operator, and owns and maintains the HAT open source code. It is the commercial arm of the HAT Foundation. To operate the HAT ecosystem on behalf of HCF, HATDeX issues SSL Certificates and GUIDs as appropriate to commercial participants and monitors the operation of the HAT Ecosystem in accordance with the HAT Code of Practice. Its commercial role includes the building and provisioning HAT Platforms and Services, making these available to individuals and organisations for participation in the HAT Ecosystem. Pre-certified HATDeX platforms and services are provided on a commercial basis to third parties.

Period this process is valid

This process is valid from the initial HAT launch in October 2016. It will remain valid until end March 2018 for anyone seeking Certification before end March 2017. The process will be up-issued before end March 2017 to reflect initial experience.

Version of this process / version history

Issue	Date	Purpose / change	Authorised
V1.0 Draft 4	18 Apr 17	Adopting to new changes after repositioning	XM
V1.0 Draft 3	19 Sep 16	Incorporating HATDeX comments	PHT
V1.0	16 Sep 16	Initial issue – draft for consultation	PHT

Contact details for HAT Certification requests

Please email

certification@hatcommunity.org for requests and information or status on certification

contact@hatcommunity.org for general information

Definitions

"Acceptable Use Policy" means HAT Acceptable Use Policy available at http://www.hatdex.org/acceptable-use-policy/.

"**AWS"** means Amazon Web Services.

"HAT-approved Application" means any third party application offering additional services to HAT Users which are approved by HATDeX on the basis of its compliance with certain requirements determined by HATDeX.

"HAT-as-a-Service" or **"HaaS"** means the following: (i) the provision of Customers with HAT Databases; (ii) the hosting of those HAT Databases on AWS; (iii) permission to access to the HAT Database through an application developed by the Customer.

"HAT Ecosystem" means the set of assets (including, though not necessarily limited to, platforms, services, applications and other products), organisations, and people, including "HAT Users," that work together to enable the privacy-preserving exchange of personal data between individuals or between individuals and organisations.

"**HAT Database**" or the **"HAT"** means the User's Hub-of-All-Things database, containing a data schema allowing for (i) the storage of data from any source without losing the structure specific to any such source; (ii) the combination of such data; (iii) the provision of a structure for third party access to such data upon authorisation of the User.

"**HATDeX"** means HAT Data Exchange Ltd, UK.

"HAT Milliner Service" means the following: (i) providing the Customer with HAT Databases; (ii) hosting those HAT Databases on the Customer's chosen platform; (iii) allowing access to the HAT Databases through an application developed by the Customer.

"HAT on Demand Service" or **"HoD"** means the following: (i) the provision of Customers with HAT Databases; (ii) the hosting of HAT Databases on AWS; (iii) permitting Customers to provide their Users with access to the Users' HAT Databases through Rumpel.

"**HAT Platform Provider**" or "**HPP**" means the provider of the platform hosting the HAT Database. HAT Platform Providers are certified by HATDeX, demonstrating that they meet required standards for privacy, security, and confidentiality.

"**HPP Third Party Services**" means all third party services necessary for HATDeX to operate as a HAT Platform Provider.

"Privacy Policy" means the HAT Privacy Policy, available at http://hatcommunity.org/privacy-policy/.

"**Services**" means the provision of the HAT Database and the provision of a platform to host the HAT Database.

"SuperUser" means a database user who bypasses all permission checks.

"User" or **"End-User"** means a user of one or more of the Services.

HAT Code of Practice and Trust Framework

The HAT Code of Practice (http://wrap.warwick.ac.uk/77858/) provides the framework for operating the HAT Ecosystem according to the following principles as held by the HAT Foundation.

First, in the economy of exchanging/trading of data, in particular personal data, the ideal way to deal with the negative externalities of personal data that face the individual, including concerns over privacy and confidentiality, is to allow individuals to claim that data from the institutions who collect and profit from it (mainly firms). While firms may also continue to hold the individual's data after the individual has claimed it for themselves, it is the aspiration of the HAT Ecosystem that when HATs are ubiquitous, firms would need only to synchronise their data with that held in individual HATs, and may not, in the future, need to an store individuals' data for themselves.

Second, the privacy of a user's information is of the utmost importance. The HAT Foundation pursues a user-centric approach to information privacy, and deems privacy to be an asset generated throughout the data journey (collection, transferal, storage, analysis and dissemination) in the personal data exchange ecosystem. The confidentiality and security issues that affect a user's personal data should be under the purview and control of the data owner – the HAT User.

Third, the HAT Foundation deems the leveraging of three forms of architecture as crucial for the development and viability of the multi-sided market: technology, activity and value.

Fourth, among the architectural forms, value co-creation for all participants is essential to drive the HAT ecosystem. Value co-creation means that the individual has the freedom to manipulate, organise, and bundle their data in any way.

Finally, the HAT Foundation regards the key to determining success for the HAT Ecosystem to be the rules of regulation and governance, including the HAT privacy principles (HAT Briefing Paper 3 http://wrap.warwick.ac.uk/65608), HAT technology (HAT Briefing Paper 4 http://wrap.warwick.ac.uk/77855), processes such as auditing and certification, and the regulatory roles of the HAT Foundation.

These beliefs are manifested and implemented in the following HAT operating principles:

HAT PRINCIPLE 1 HAT Personal Data is owned by the HAT User

HAT PRINCIPLE 2 Access to HAT User Personal Data is controlled by the HAT User

HAT PRINCIPLE 3 Usage of HAT Personal Data is controlled by the HAT User

HAT PRINCIPLE 4 The Value of the HAT Marketplace is driven by the HAT Participants

HAT PRINCIPLE 5 HAT-ready Devices, HAT-ready Services and HAT Service Providers must be HAT Compliant, supporting the other HAT Principles implemented by the HAT Information Policies

Information Policies

Ten HAT Information Policies support the five HAT operating principles. These are the key features of the HAT Trust Framework and the Terms of Use of the HAT. The HAT Information Policies are necessary for all HAT Participants to successfully implement the HAT vision. The HAT Information Policies define the responsible actions and outcomes required by HAT Service Providers in order to achieve HAT Certification. The specific HAT Information Policies that implement the HAT Principles

are the following rules. These policies apply to HAT roles such as HAT Platform Providers (HPPs), HAT Application Providers (HAPs), HAT Developers and other HAT Service Providers (HSPs).

HAT INFORMATION POLICY 1 – Definition Of Personal Information & Usage Data

The data defined as personal data will be described by a HAT personal data use taxonomy. This taxonomy will define what data will be stored and collected by the HAT User and recorded by the HAT on the behaviour of the HAT User.

HAT INFORMATION POLICY 2 – Audit & Charging

The personal data use taxonomy will be an auditable record that will be visible to a HAT User. A HAT User will be able to see the usage of their HAT Data by HAT Service Providers. A HAT User will be able to access the audit record of their HAT Data, including a record of HAT-to-HAT Service transaction exchanges. A HAT Service Provider can record all HAT transactions collected or generated for a HAT User. A threshold can be set for how the HAT transaction may be chargeable by the HAT Service Provider.

HAT INFORMATION POLICY 3 – Visibility Of Data & Services

A HAT User will be able to control the visibility of HAT Personal Data to other HAT Users and/or HAT Service Providers. A HAT Service Provider may make their HAT Services visible to one or many HAT Users, but only HAT Personal Data that has received explicit consent from the HAT User, the owner of that data, may be seen. This is to enable visibility to the HAT Ecosystem of HAT Services, HAT Devices and HAT Service Providers, Applications, and Users (within the conditions of the HAT User's consent to access and use their personal data).

HAT INFORMATION POLICY 4 – Personal Data Access Control

Definition of Access. Access means "View only HAT Data" – A person can control access to their personal HAT data, controlling what is transmitted from or to other parties. This access control is provided by the HAT Service Provider to the HAT User over their HAT Data.

HAT INFORMATION POLICY 5 – Personal Data Usage Control

Definition of Usage. Usage means "able to add, update and change HAT Data" – A person can control their personal HAT Data use for a general or specific usage scenario for matching and general use. For example, the control of the use of HAT Personal Data that is for general sharing or private to access and use by HAT Service Providers, such as general interests and services. Additionally, this includes scenarios that involve specific personal data usage and choices for a HAT User, for example HAT User activity, user-specific preferences, likes, and dislikes to share with HAT Providers.

HAT INFORMATION POLICY 6 – Personal Authorisation Control

Definition of Authorisation. Authorisation means "able to set a permission level" – A person can control the access to and use of their HAT Data by controlling the authorisation governing its use. The HAT Service Provider will provide opt-in and opt-out choices for HAT User authorisation permissions of their HAT Data.

HAT INFORMATION POLICY 7 – Personal Data Release & Notification Control

Definition of Release. Release means "able to control what is broadcast as notification" – A person can control the release of their HAT data to HAT Users and HAT Service Providers. The HAT Service Provider enables the HAT User to control the release of what HAT Personal Data is made available to HAT Service Providers. Notifications will be provided to the HAT User of when HAT Data has been accessed and used by the Hat Service Provider and between HAT Services transactions, including any

security violation notifications of HAT Data that may affect the HAT User. HAT Personal Data that is shared and used will be subject to the HAT User Authorised Permissions.

HAT INFORMATION POLICY 8 – Personal Data Security

A HAT user is able to determine the security of their personal data by the HAT Service Provider that is hosting their HAT Data. This includes safeguards for managing HAT Personal Data, such as firewalls and data encryption, physical access controls to HAT data centres, secure transmission and information access, authorisation controls, and monitoring, detection, notification, escalation and prevention of fraud and misuse of HAT Data.

HAT INFORMATION POLICY 9 – Personal Data Geolocation

All personal HAT geolocation data tagging must be visible and controlled as an option of anonymity by the personal HAT User as part of the HAT personal authorisation permissions.

HAT INFORMATION POLICY 10 – Personal Data Removal

HAT Data is to be removed after transactional use by the HAT Service Provider. The HAT Service Provider conducts data sanitation to ensure that a HAT User's data privacy is maintained after their data is used by HAT-ready Devices and HAT-ready Services. HAT Data that ceases to be hosted by a HAT Service Provider is removed from their HAT hosting service and is no longer accessible by that HAT Service Provider. HAT Data may only be retained in compliance with local legal requirements.

HAT Certification Process - principle features

Purpose and responsibilities

For Certification to be granted by HCF, it is required that any and all applicants agree with, and comply to, the requirements detailed in Appendix A, Appendix B (if applicable), and Appendix C.

Certification of participants in the HAT Ecosystem, in accordance with this process, is needed to ensure the principles of the personal data marketplace are upheld by all involved, for the benefit of all. This is to promote visibility, simplicity, interoperability and trust as key features of the HAT Ecosystem.

Assets are put into the HAT Ecosystem by HAT Platform Providers (HPPs) and Hat Service Providers (HSPs), which need to be Certified to do so in accordance with this process. It is presently intended that self-certification, subject to audit by the HCF, will cover this process.

Key HAT Certification responsibilities

HAT Service Providers (HSPs) provide a vital role in provisioning, hosting, and supporting HAT personal data platforms so that the HAT User's data remains private, confidential, and secure, and is shared only with the data owner's express permission, within the ecosystem trust framework established by this procedure.

HAT Application Providers (HAPs) are key to the development of HAT User software for platforms and services that enable personal data to be managed and associated with benefits for HAT users and HAT providers.

HAT Community Foundation (HCF) is an independent Members' body representing the HAT user community. It exercises oversight and governance of the HAT Ecosystem, and HATDeX

operation of the Ecosystem, overseeing in particular the application of this certification process. HCF also advises HATDeX on the distribution of benefits back to the community.

HCF operates the HAT ecosystem and its community of the users, HAPs, and HSPs that are engaged in the HAT marketplace to ensure that the principles of the HAT are maintained for the benefit of the HAT community. This work includes:

- Owning and maintaining the open source software (formally adopting community-developed changes and managing versioning of the software assets)
- Advising prospective HPPs and HSPs on Certification
- Supporting (in commercial terms) the development of prospective HAPs' and HSPs' development of new platforms and services for the HAT Ecosystem, and licensing HATDeX-developed assets in support
- Undertaking Certification audits in accordance with this procedure
- Issuing SSLs and GUIDs as required to Certified agencies (HAPs and HSPs)

HAT Data Exchange Ltd (HATDeX)'s primary role is to offer data exchange capabilities that facilitates exchange by executing the Data Debit between an individual HAT and another entity. HATDeX may also act on behalf of HCF, to execute certain HCF functions for the ecosystem, for example utilising MarketSquare services for listing all certified apps, providers, and statistics. HATDeX's main services include:

- HAT Onboarding Capability
- Financial clearance for entities within the ecosystem
- Data Exchange processes and statistics
- Trading Capability

Collecting and monitoring meta-data for all data transactions in the HAT Ecosystem ensures appropriate us, noting community determination of appropriateness. Neither HCF, HATDeX, nor any HAPs or HSPs have any access to any of the personal data stored within an individual user's HAT.

HATDeX is also an HAP and an HSP in its own right, providing a range of platforms and services built for HAT. These HATDeX platforms and services are developed from the open source software and are intended to promote expansion of the ecosystem. They can be made available on commercial terms to any other organisation wishing to become an HAP or HSP - using, for example, "HAT as a Service" (HaaS).

Together, HCF, HATDeX, Application and users constitute the HAT ecosystem and represent the HAT marketplace and services that enable the HAT User Community to exist and grow, increasing the benefits to all.

HAT Certification Process

Anyone seeking Certification must be a member of the HAT Foundation. Submission may be subject to audit by HATDeX, working as agent on behalf of the HCF.

Informal / optional steps:

1. Prior to formally submitting answers and evidence against Appendix A, B and C those entities interested in seeking Certification may wish to open discussion with HCF regarding the use the HAT APIs, schema and logic. HCF may appoint HATDeX to directly engage in such activities. Alternatively, prospective applicants may wish just to download the open source code and start development without consultation.
2. Following initial informal consultation and/or use of the open source code, applicants may wish to enter into an use agreement with HATDeX to ensure that the prospective HAP/HSP is consulted/informed about any prospective changes the codeset or APIs.
3. Once HCF (and the prospective applicant) are satisfied that a prospective HAP/HSP is using the open source code correctly, that metadata is being reported to HCF, and that interoperability has been achieved, the HCF will recommend that the HAP/HSP is ready for Certification through the formal process (see below). Note that this may result from a commercial agreement to buy a HATDeX business solution – such as "HAT as a Service" (HaaS).

The formal process is then to:

1. Applicants (prospective HAPs or HSPs) should complete and sign the self-certification check-list at Appendix A, providing supporting evidence as appropriate, and submit this to HCF by email: certification@hatcommunity.org
2. Applicants may then be subject to audit by HCF – this will be a "light-touch" telephone/Skype or email-based review of the applicants responses and evidence
3. Subject to satisfactory responses to step 2, the Applicant will need to join the HAT Foundation as an Associate or Full Member (if not already a member) following which HCF will issue the Certificate of Conformance
4. Once Certified, the Applicant can apply to HCF for SSLs and GUIDs as appropriate.

This process is valid from the initial HAT launch in October 2016. It will remain valid until end March 2018 for anyone seeking Certification before end March 2017.

Sources of information for the HAT

Current website:

http://hatcommunity.org

Technology:

http://hubofallthings.com/hatoutputs/tech-outputs/

http://forum.hatcommunity.org

https://github.com/Hub-of-all-Things/HAT/blob/master/README.md

API documentation can be found at http://hub-of-all-things.github.io/doc/

Security (practice example):

http://www.hatdex.org/volume-1-issue-2-17-june-2016/

Appendix A
HAT Certification Check List

Any natural person or corporate body must be certified in accordance with the HAT Code of Practice before they can contribute assets to the HAT Ecosystem, including but not limited to platforms, services, applications and other products. Certification requires agreement to or compliance with the requirements listed in the certification check-list below. Anyone seeking certification shall submit answers and supporting evidence to HAT Community Foundation (HCF) in confidence that their responses by be audited by HATDeX (working on behalf of the HCF) before being issued a Certificate.

ID	Requirement	Check / Evidence
1	**Ecosystem and Legal Requirement**	**N/A**
1.01	You agree to all HAT Users collectively monitoring Service Providers (application and hosting), and agree that they can report any breach of compliance with the HAT Code of Practice.	
1.02	You agree that HAT Community Foundation (HCF) Certification is required for any organisation to operate in the HAT ecosystem, prior to obtaining an SSL.	
1.03	You agree to support the HAT Ecosystem Design: http://hatcommunity.org/the-hat-ecosystem/.	
1.04	You agree to comply with all applicable laws, including all the applicable data protection laws.	
1.05	You agree to grant HCF the right to conduct any activity necessary for the maintenance and support of this Certification procedure, including this checklist.	
1.06	You agree to notify HCF promptly of any misbehaviour in the Ecosystem and any other breach of security.	
1.07	You agree to not sell, resell or lease the HAT Services or use them in any manner that could lead to physical damage, death or personal injury.	
1.08	You agree to bear responsibility for responding to legal requests for information on your End-Users, such as search warrants or court orders.	
1.09	You agree to contact HCF with regard to legal request only if you have no access to the requested information, HCF will review and respond to legal requests in accordance with its Government Request Policy.	
1.10	You recognise and agree that if you fail to respond to legal requests, the HCF has no obligation to respond.	
1.16	You recognise HATDeX as the HAT scheme operator, owner and maintainer of the HAT open source codes, and the commercial arm of the HAT Foundation.	

2	**Commercial Requirement**	**N/A**
2.01	You agree that you are responsible for your conduct and the conduct of your End-Users on the HAT and for the content of the data that you or your End-Users upload, copy, download or share.	
2.02	You agree to cooperate with HCF, when this is necessary to investigate service outages or alleged breaches of this checklist or the applicable law.	
2.03	You agree that HCF may use your feedback or suggestions and your End-Users' feedback or suggestions without any obligation to compensate you for them.	
2.04	HCF may provide you with aggregated ecosystem information, including information on the total number of HATs in the network, the most popular data being shared, and the amount of data coming in and going out of the HATs of your End-Users. Such aggregate information enables others to build services on the HAT network and offer benefits for you. For the purposes of providing this information, you authorise HCF to log all the metadata generated by the data entering and leaving your End-Users' HATs. The collection of such metadata enables HCF to identify the types of data coming in and leaving the HAT but does not allow it to identify your End-Users in any manner whatsoever.	
	Your obligations concerning your relationship with your End-Users	**N/A**
2.05	You agree to include as a minimum the terms in Appendix C within all End-User agreements whether made by you or by any intermediaries offering your services to End-Users.	
2.06	You agree that you will share your End-Users' data stored on their HATs with third parties only when they authorise you to do so through application settings or data debits. You also agree that you will enable your End-Users to withdraw their authorisation to share their data with any third party at any time. When your End-Users withdraw their authorisation, you will immediately stop any unauthorised sharing.	
2.07	You agree that you will not access or scan your End-Users' data stored in their HATs unless required to do so by the law.	
2.08	You agree to adopt a privacy policy informing your End-Users on how you comply with applicable data protection laws, the information you collect from your End-Users, the purposes of collecting such information, the third parties with whom you share such information and the security measures you adopt.	
2.09	You agree to notify your End-Users of any unauthorised use of their HAT PDMAs and any other breach affecting the security of their HATs.	

2.10	You agree to inform your End-Users on the rights and obligations deriving from the creation and use of their HAT Accounts by publishing all your applicable legal agreements and policies on your website.	
2.11	You agree to inform your End-Users of any change to your applicable legal agreements and policies.	
	Suspension of your End-Users' hat account and termination of your legal agreements with them	**N/A**
2.12	You agree that you will suspend an End-User's HAT PDMA only in one of the following conditions: a. you reasonably believe that the End-User acted or is acting in violation of any applicable law or the legal agreements applicable between you and the End-User; b. you reasonably believe that the HAT Account of the End-User has been accessed by an unauthorised third party or its security has been compromised in any other manner; c. the suspension is necessary to protect your network, customers, commercial interests or any other essential interest; d. if you are required by law or by a governmental authority to suspend a HAT account.	
2.13	You agree to give your End-Users reasonable advance notice of a suspension and offer them the opportunity to cure the grounds underlying the suspension.	
2.14	You have the right to terminate your agreements with your End-Users for the provision of HATs only in the following conditions: a. the termination is in accordance with the terms of the legal agreements between you and your End-Users; or b. the termination is required by the law or a governmental authority.	.
	Ownership and rights on your End-Users' data	**N/A**
2.15	You agree that when your End-Users upload their data on their HATs, they will continue to own such data.	
2.16	You agree that when your End-Users upload their data on the HAT, you will not acquire any right on such data, with the following exceptions: a. the right to share your End-Users' data when they choose to do so; b. the exercise of any right necessary to allow your End-Users to access their HATs; c. the exercise of any right on your End-Users' data that is necessary for the maintenance and support of the HAT.	
	International data transfers	**N/A**

2.17	If you transfer your End-Users' data internationally, you agree to adopt all necessary measures to comply with all applicable laws on international data transfers.	
	Administration of the hat accounts	**N/A**
2.18	You agree that HCF bears no responsibility for the internal administration of your services. You are responsible for ensuring the security of administrator accounts and HAT Accounts of your End-Users, while you act as administrator for the HAT Accounts of your End-Users. You may deploy, maintain, backup, delete, monitor, suspend or terminate the HAT PDMAs of your End-Users.	
	Third-party services	**N/A**
2.19	If you use a third party service, such as a service that uses a HAT Application Programming Interface (API), you are solely responsible for the conduct of such third party in relation to the provision of such third party service.	
2.20	You agree to HCF bears no responsibility for the conduct of such third party, including third party access to or use of your data and your End-Users' data. HCF does not offer support for any service provided by the third party.	
3	**Technical Requirement**	**N/A**
3.01	Do you host HAT in one of the following cloud infrastructure – AWS, Microsoft Azure, and IBM Bluemix (exempted from next question).	
3.02	If not, please specify your security policy using alternative options: https://docs.google.com/spreadsheets/d/1ZLdwevIh2Xhzje1kbH3G-XHs3ivRWDDGpTcP86NEfY4/edit?usp=sharing	
3.03	You agree that MarketSquare may act as an additional trust anchor for third party applications. Note – by default, no third party application can add data to or request data from a HAT through a Data Debit without an approved account on an individual HAT. In order to create an account (and obtain approval) on a HAT, a third party application must go through MarketSquare. (This is not to create and approve Data Debits or other data transactions). MarketSquare enforces the following process to provide such a trust anchor: • An application developer must retrieve a JWT crypto-signed token from MarketSquare when they register an application (e.g. data plug) and include that in the application's configuration. • Once the app is registered, it provides MarketSquare with its hash (oneway encrypted password, using BCrypt algorithm), which will then be given by MarketSquare to the HAT when the app creates an account. • The app can ask for access to a specific HAT by requesting MarketSquare (via	

	an API call) to create an account on the HAT, providing the token to prove its identity. • Upon successful account creation, the app can directly log into the HAT to retrieve the HAT's token (as in the first item above), using the password known only to the app, which corresponds with the encrypted value provided to the HAT via MarketSquare. In the current release of the HAT, all external user accounts (such as marketers and application providers) will be verified and approved or rejected by the administrators of MarketSquare, as will all Data Offers and applications.	
3.04	Your services ensure communication between any client and any HAT must go through the designated APIs. This includes the activities of the HAT owner managing their personal data through any data browser.	
3.05	Your services ensure SSL-encrypted communication is required between any client (apps, MarketSquare or Rumpel) and any HAT.	
3.06	Your services ensure token-enabled authentication with the HAT and service provider verification to enter the ecosystem from MarketSquare.	
3.07	Your services ensure Activating Direct Data Debit transactions requires the HAT user's review and approval.	
4	**If your organisation is to become an HPP – Hosting HATs**	**N/A**
4.01	Your services ensure that When provisioning a HAT database, the temporary administrator account to create a hat needs to be immediately deleted upon successful HAT launch.	
4.02	Your services ensure that the provisioning mechanism must treat HATs as generic containers, without internal knowledge or exposure to how they operate.	
4.03	Your services ensure that encryption key management infrastructure is in use. Encryption key generation, exchange and storage are distributed for decentralised processing.	
4.04	Your services ensure that each HAT stores its data in its own, separate database instance.	
4.05	Your services ensure that each HAT uses the most up to date schema stated at https://github.com/Hub-of-all-Things/HAT/blob/master/README.md	
4.06	Your services ensure that each HAT is only accessible by the single designated HAT account.	
4.07	Your services ensure that your services ensure that each HAT database is isolated at the server level (isolated as virtual machines or containers).	

4.08	Your services ensure that the Super-User account on the database engine should be inaccessible, and is only reachable from inside a secured Server or Virtual Machine (VM).	
4.09	Your services ensure that Super-User account on the database engine should never be used or accessed for administrative or other purposes by provisioning systems or administrators.	
4.1	Your services ensure that Each HAT Database should be encrypted.	
4.11	Your services ensure that Each HAT Database is backed up at least once a week.	

To be completed by the applicant:

I /we hereby warrant that responses to the above questions are to the best of my knowledge correct, that any additional evidence submitted in support of the answers above is correct, and that I/we will continue to operate within the HAT Ecosystem in accordance with these answers and the wider Code of Practice and Trust Framework on which these requirements are based.

Signed:

Name:

Capacity:

Date:

Appendix B
HAT Certification Check List - addendum

The following requirements are in addition to those of Appendix A for non-standard platform hosting solutions (hosting solutions other than AWS, Microsoft Azure, and IBM Bluemix):

ID	Question / requirement	Minimum Standard or recommended best practice
1	**Technical requirements**	Please note that where a specific standard, protocol or manufacturer program is referenced below, the HCF will consider an equivalent to that stated, however it is the responsibility of the Participating Party to demonstrate the equivalence. Should this equivalence not be satisfactorily demonstrated, the HCF reserves the right to score accordingly and may result in a sub satisfactory score.
1.10	**Encryption**	
1.11	What encryption standards are used when storing data at rest?	AES256, PGP, FIPS 140-2 (desirable for personal data, essential for sensitive data)
1.12	What encryption standards are used for data in transit?	AES256, SMIME, SCP, SSL (essential for personal and sensitive data)
1.13	Is data ever stored in an unencrypted form?	No
1.20	**Server Password Policy**	
1.21	Define you password strength policy.	Minimum 8 characters, upper, lower case and special characters are mandatory
1.22	What encryption is used to secure username/password login?	https (128bit), ssh, AES256
1.30	**Server and Network Management**	
1.31	How often are servers penetration tested?	Annually, every 6 months
1.32	How often are the servers patched?	Monthly
1.33	What is the firewall policy (specify all open ports)?	Default deny, only essential ports open
1.34	What Intrusion Detection devices are in use?	SNORT, Cisco, Juniper

1.35	How are network and virtual machines segregated?	VLANs, VM isolation
1.40	**Antivirus**	
1.41	What Antivirus solution is in place?	Symantec, Kapersky
1.42	How often are the antivirus signatures updated?	Hourly, daily
2	**Data Protection and Information Security**	
2.10	**Data Protection Act**	
	Please confirm that your organisation has Data Protection Registration to cover the purposes of analysis and for the classes of data requested	Should be confirmed by all suppliers and contractors
	Please describe the content of any Data Protection training provided to your staff; how regularly it is provided and updated, and to whom it is provided.	Details of regular training (face to face, best practice guidelines for staff, clear procedures)
	Who is the Data Protection Officer or Caldicott Guardian (if NHS)?	Named contact
2.20	**Data Audit and Access Control**	
	What audit logs for access and deletion of data are available?	All access is logged
	How long are audit logs kept for?	Logs are kept for 6 months
	What data erasure/data retention policies and procedures are in place?	Would expect to see mention of cross shredding and confidential waste process for paper records, shredding of DVDs/CDs, wiping if external storage media (such as USB sticks) with a suitable software tool, sufficient protection of media which cannot be wiped initially. Financial data should be wiped to PCI DSS standards.
	What information security and audit measures have been implemented to secure access to, and limit use of information within your organisation?	Information Security Policy, training and guidance for staff, procedures and specific technology used, ISO27001 (preferred industry standard)
2.30	**Data Security**	
	What physical security arrangements are in place where this data is to be processed and stored?	Access to site, requiring authorised key or card entry – audit logs available for when entry/exit has occurred. Key or

		card access only available to employees that need access to the physical site.
	What user privilege control is in place?	Least privilege principle is in place
	What information is shared regarding data breaches and near misses?	The University should be informed of any data breaches and near misses and clear processes should be in place to prevent and act upon a data breach.
	What procedures are in place for investigating security breaches?	Internal investigation team, outsourced to third party
3	**Business Continuity**	
	What continuity plans are in place to cover loss of staff resource and expertise	Staff cover plans and details of impact of service delivery
	What continuity plans are in place in the event of loss of or severe disruption to/loss of premises	Identification of alternative premises, defined timescales for recovery
	When was the business continuity/disaster recovery plan last tested	Some form of annual testing would be preferred (either desktop or real life test)
	What data back-up procedure is in place and encryption?	Nightly backups taken, stored off site, encryption - AES256, PGP
	What are the recovery timescales?	The acceptability of the stated recovery timescales would depend in the needs of the user and should be determined by user groups
4	**Additional Data Protection Terms**	
	Physically, where is the data kept? Is it ever located outside of the UK / EU? - INFORMATION ONLY	Require confirmation of where all data (including primary and back up data) is hosted, stored, processed, used or disposed of
	Please complete appropriate section of Add'l Data Protection Terms Tab - MANDATORY	Require signature of appropriate Additional Data Protection Terms and Conditions (see tab) depending on physical location of data

Appendix C
HAT Certification Check List – standard End-User Terms

HAPs and HSPs shall agree to use the following terms and conditions within end-user agreements:

ID	Requirement
1	**Obligations concerning your relationship with your end-users**
1.01	You agree that you will share your End-Users' data stored on their HATs with third parties only when they authorise you to do so through application settings or data debits. You also agree that you will enable your End-Users to withdraw their authorisation to share their data with any third party at any time. When your End-Users withdraw their authorisation, you will immediately stop any unauthorised sharing.
1.02	You agree that you will not access or scan your End-Users' data stored in their HATs unless required to do so by the law.
1.03	You agree to adopt adequate security measures to protect your End-Users' data stored in their HATs.
1.04	You agree to adopt a privacy policy informing your End-Users on how you comply with applicable data protection laws, the information you collect from your End-Users, the purposes of collecting such information, the third parties with whom you share such information and the security measures you adopt in accordance with paragraph 3 of this Article.
1.05	You agree to notify your End-Users of any unauthorised use of their HAT Accounts and any other breach affecting the security of their HATs.
1.06	You agree to inform your End-Users on the rights and obligations deriving from the creation and use of their HAT Accounts by publishing all your applicable legal agreements and policies on your website.
1.07	You agree to inform your End-Users of any change to your applicable legal agreements and policies.
2	**Suspension of your End-Users' HAT PDMA and termination of your legal agreements with them**
2.01	You agree that you will suspend a End-User's HAT PDMA only when: a) you reasonably believe that such End-User acted or is acting in violation of any applicable law or the legal agreements applicable between you and the End-User; b) you reasonably believe that the HAT Account of such End-User has been accessed by an unauthorised third party or its security has been compromised in any other manner;

	c) the suspension is necessary to protect your network, customers, commercial interests or any other essential interest; or d) if you are required by law or by a governmental authority to suspend a HAT account.
2.02	You agree to give your End-Users reasonable advance notice of a suspension and offer them the opportunity to cure the grounds underlying the suspension.
2.03	You have the right to terminate your agreements with your End-Users for the provision of HATs only when: a) the termination is in accordance with the terms of the legal agreements between you and your End-Users; or b) the termination is required by the law or a governmental authority.
3	**Ownership and rights on your end-users' data**
3.01	You agree that when your End-Users upload their data on their HATs, they will continue to own such data.
3.02	You agree that when your End-Users upload their data on the HAT, you will not acquire any right on such data, with the following exceptions: a) the right to share your End-Users' data when they choose to do so; b) the exercise of any right necessary to allow your End-Users to access their HATs; c) the exercise of any right on your End-Users' data that is necessary for the maintenance and support of the HAT.
4	**International data transfers**
4.01	If you transfer your End-Users' data internationally, you agree to adopt all necessary measures to comply with all applicable laws on international data transfers.
5	**Administration of the HAT PDMAs**
5.01	You may act as administrator for the HAT PDMAs of your End-Users. You may deploy, maintain, backup, delete, monitor, suspend or terminate the HAT PDMAs of your End-Users. HCF/HATDeX bears no responsibility for the internal administration of the Business Services. You are responsible for ensuring the security of administrator accounts and HAT PDMAs of your End-Users.
6	**Legal requests**
6.01	You are responsible for responding to legal requests for information on your End-Users, such as search warrants or court orders.
6.02	You will contact HCF with regard to legal request only if you have no access to the requested information.

6.03	HCF will review and respond to legal requests in accordance with its Government Request Policy.
6.04	If you fail to respond to legal requests, HCF/HATDeX has no obligation to respond.