TagItSmart!
Smart Tags driven service platform for enabling ecosystems of connected objects

Grant agreement 688061

Circular economy for electronics reuse

Deliverable ID:	**D 2.1**
Deliverable Title:	System architecture and design
Revision #:	**v2.0**
Dissemination Level:	**Public**
Responsible beneficiary:	TagITSmart! Consortium
Contributing beneficiaries:	
Contractual date of delivery:	30.3.2018
Actual submission date:	19.09.2017

Start Date of the Project: 1 January 2016 Duration: 36 Months

PROPRIETARY RIGHTS STATEMENT
This document contains information, which is proprietary to the TagItSmart! Consortium. Neither this document nor the information contained herein shall be used, duplicated or communicated by any means to any third party, in whole or in parts, except with prior written consent of the TagItSmart! consortium.

Contents

Introduction ***4***

Section 1 - Definition of the System architecture ***4***

1.1 eReuse.org Workbench **4**

1.2 eReuse.org Devicehub **5**

1.3 Global Record of Devices **7**

Section 2 - Explanation of the work carried out and overview of the progress ***9***

1.4 The final Tag proposal **13**

1.4.1 User experience 13

1.4.2 Tag proposal 14

Section 3 - Conclusions ***15***

Section 4 - References ***16***

Section 5 - Annex ***16***

1.1 Devicehub technical tag specification **16**

1.1.1 eTags 16

1.1.2 Tag ID design 16

1.1.3 Creating tags 17

1.1.4 Linking a tag 17

1.1.5 Getting a device through its tag 17

1.1.6 Tags and migrations 17

1.1.7 Use-case with eTags 17

Approvals

	Name	Organization	Date	Visa
Project Management Team	Leandro Navarro	Pangea	19/9/2018	L.N.

Document history

Revision	Date	Modification	Authors
v0.1	25/2/2018	First draft (Padua meeting)	David Franquesa, Xavier Bustamante, Leandro Navarro
v0.2	15/2/2018	Ready for revision	Xavier Bustamante
v0.3	18/2/2018	Consistency check and final reading	David Franquesa
v1.0	20/2/2018	The first version of the deliverable	Xavier Bustamante
v1.1	2/7/2018	Update with section I "Definition of the System architecture" with the last system release and section II with the work carried out.	Xavier Bustamante
v1.2	3/7/2018	Second draft	Xavier Bustamante
v1.3	5/7/2018	Ready for revision	Xavier Bustamante
v1.4	8/7/2018	Consistency check and final reading	David Franquesa
v1.5	9/7/2018	The second version of the deliverable	Xavier Bustamante
v2.0	19/09/2018	The revised version of the deliverable	Xavier, David, Leandro

Introduction

We have augmented the eReuse.org software ecosystem with the usage of the TIS tags and Everythng, resulting in the architecture we present in this deliverable.

There are three main softwares in the eReuse.org ecosystem:

1. The Workbench, which is a suite of tools refurbishers use to refurbish devices to reuse by obtaining their metadata, benchmarking them, erasing their private information, etc;

2. The Devicehub, a distributed Device Management System on the cloud that several actors use to manage the devices, tag them with TIS tags, and exchange them.

3. The Global Record of Devices (GRD), a centralized shared cloud that this project aims to build in Everythng that ensures global traceability, avoids leakage, and generates circularity metrics by recollecting non-private metadata from devices.

Section 1 - Definition of the System architecture

The eReuse.org architecture is a distributed multi-agent system implemented as software services, tools, and data repositories, with the main objectives of: (1) managing reusing and recycling of devices, (2) contributing in ensuring reuse and recycle by supporting traceability, (3) facilitating third parties to join eReuse.org's effort by using, extending, and integrating the system, (4) maximizing the use of devices, and (5) generating inputs for the indicators that measure circularity.

The following sections describe the three softwares in detail:

1.1 eReuse.org Workbench

The eReuse.org Workbench is a toolset that assists in registering, refurbishing, and tracking devices. It captures hardware characteristics (like the serial number) of devices and their components, rates the devices, securely deletes data, and installs GNU/Linux OS when possible.

The tools of Workbench are:

- Workbench computer. A software that executes on a computer and, without human interaction, automatically executes the following tools:

  - Hardware discover. Obtains metadata from the computer and its components, including ways of identifying a device and information for traceability, reusing, and generating circularity inputs.

  - Eraser. Deletes private information from data storage units by performing standardized erasure methods that users can parametrize.

  - Benchmarker. Rates the capacity of the computer and its components in order to value them.

  - Tester. Performs quality tests to guarantee the capacity of the machine to operate correctly and without failure.

    - GNU/Linux OS installer: installs a GNU/Linux OS with preselected software and configuration.

- Workbench Server. A software that manages executing the Workbench PC on multiple devices (up to hundreds) through a local network. Workbench Server is usually served through a Box, a mini-computer that acts as the point of management in the warehouse when preparing devices to reuse.

- Android App. A smartphone and tablet Android app that has two functionalities:

    - Obtain metadata from devices that are not computers, like peripherals or electrical appliances, by scanning their barcodes and taking pictures from them.

    - Link devices with tags generated by the eReuse.org tools, like Tag IT Smart tags with QR codes and NFC chips.

- Photobox. A machine that assists in rating the appearance of a device by taking pictures from devices from different views, like frontal, sides and rear. A developing AI can detect scratches and imperfections from the pictures and automatically rate the devices.

When refurbishing a device for reuse, operators process them through the eReuse.org Workbench, executing the tools that they see fit for the type of device, and finally the Workbench Server generates a reuse report containing all the gathered information. This report is then uploaded to the distributed cloud software; the eReuse.org Devicehub, which we explain in the next section.

The Workbench toolset is developed in Python 3 and Android with open-source technologies and operative systems such as Debian 9 over PCs and Raspberry Pi.

1.2 eReuse.org Devicehub

The eReuse.org Devicehub is a distributed Device Management System (a type of IT Asset Management System), offered as a web app and focused in efficiently managing the circular life-cycle of devices –reusing and recycling.

Our main objectives are:

- To offer a common IT Asset Management for donors, receivers and IT professionals so they can manage devices and exchange them. This is, reusing –and ultimately recycling.

- To automatically recollect, analyse, process and share (controlling privacy) metadata about devices with other tools of the eReuse ecosystem to guarantee traceability, and to provide inputs for the indicators which measure circularity.

DeviceHub recollects devices from the reports of the eReuse.org Workbench and other integrated systems and manages their full workflow, logistics, and tracking –the latter one connecting to the eReuse.org global traceability system, we call Global Repository of Devices (GRD), which we explain in the next section. Devicehub manages and prints certificates and customer-friendly reports, it manages lots of devices, and it can design and print smart tags with QR and NFC technologies that boost efficiently and avoid leakage.

Devicehub are federated and autonomous, and interact with external systems (like other Devicehubs) to manage the different processes involved in reusing and recycling, like disposal or external reusing.

The main characteristics of Devicehub are:

- Management of devices: manages the asset identification process and the life span of the devices of the organization, the workflow, and external ones over which the organization has control.
- Reports: generates automatic personalized reports and analytics, being able to ensure compliance, detecting critical aspects, such as loss of devices, over assignment of resources, etc. Reports can be PDF documents or spreadsheets.
- Certifications: saves, manages, and exports certificates, such as the results of the tests and deletion of the hard-drives, being able to answer to audits and show it to end users.
- Tag management: designs and generates tags used to track the devices by using the utility eReuse.org tag. These tags are linked (associated) to devices, and they can travel between Devicehubs while keeping accountable records. Tags can be generated in two ways: directly through a label printer that the user has, or by requesting the tags to a Tag IT Smart (TIS) manufacturer. In the second case, Devicehub integrates with the tag manufacturer by generating the information it needs in order to print the tags and registering the new tags back.
- Logistics, traceability, and tracking: manages the transportation of devices by mapping their coordinates to places and assigning transporters and destinations.
- Compliance management: sets compliance rules to lots of devices and reacts when irregularities happen or when they break. Compliance can be shared between Devicehubs.
- Device rate and selling price: rates the devices according to the benchmarking and testing reports of the Workbench, taking into account performance, functionality, and aesthetics. Finally, it suggests a parametrizable range of prices.

Devicehub is split into two technical subprojects:

- Devicehub: a RESTful Python 3 web application built on the microframework Teal, an open-source micro-framework we are building too as part of this Devicehub; Teal is built on Flask and uses PostgreSQL as database.
    - The old Devicehub is built on python-Eve and Flask, and uses MongoDB as database.
- DevicehubClient: a browser app built using Javascript, CSS, and HTML on the framework Angular.

Devicehub uses a tool software called Tag that we are building as a helper tool when ordering tags to TIS tag manufacturers and when managing TIS tags between Devicehubs, as a way to keep a centralized traceability of the tags.

1.3 Global Record of Devices

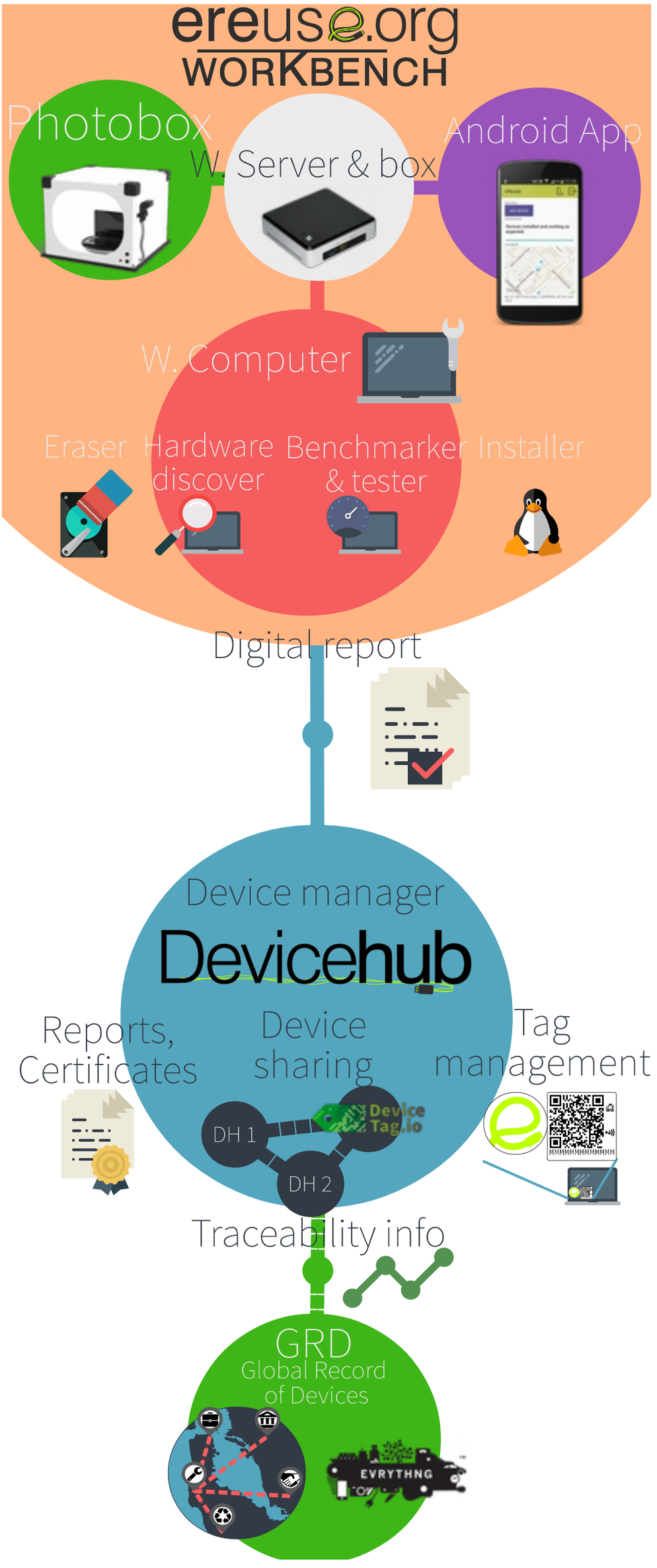
The Global Record of Devices (GRD) is an auditable (and replicable) online log that maintains a global list of traceability information about devices, so it can assist when there is leakage or similar problems. The GRD works with open-data and is designed to be used with external users who want to report traceability information. At the same time, GRD aggregates traceability data with the objective of using this data as inputs for indicators measuring circularity indicators. It is comparable to a distributed blockchain.

GRD provides a REST API to allow ITAMS, as DeviceHub, to report the life cycle of devices, environmental responsibilities for organizations, etc. It collects from each device, at least, the geographical paths it has followed (not in detail to preserve privacy), the DeviceHub where it has been stored, the collection points where it was located before its final recycling and, in the case of computers, the record of its components.

The main differentiator with competitors (freshservice.com, device42.com, and GPLI for open-source solutions) is traceability throughout the life-cycle.

GRD exists as a prototype and it is the aim of this project to build it using [1] Everythng.

The following diagram represents the three main components of the systems and how they interact with each other:


ereuse.org
WORKBENCH
Photobox
W. Server & box
Android App
W. Computer
Eraser
Hardware discover
Benchmarker & tester
Installer
Digital report
Device manager
Devicehub
Reports, Certificates
Device sharing
Tag management
DH 1
DH 2
Device Tag.io
Traceability info
GRD
Global Record of Devices
EVRYTHNG

Section 2 - Explanation of the work carried out and overview of the progress

The main activities carried out in this task have been of three types: 1) design and test the tags we need for our use case, 2) develop the eReuse.org software modules for compatibility and integration with the TIS modules, and 3) develop and test the eReuse.org software modules to implement the use case of a *Circular Economy* of *slow moving* circular goods (SMCG), generating their corresponding user stories to meet the new requirements. These are some of the activities carried out grouped by subactivities.

The eReuse modules must develop new features coming from our SMCG use case and from the capabilities provided by the SmartTags and the TIS platform. We can summarize our new epics/features to implement as follows: 1) identify uniquely the devices using NFC tags, 2) set non operative and operative devices by certified refurbishment tests, 3) ensure devices quality in refurbishment protecting brands image and consumers, 4) selling price and value of use of used devices is transparent to end-users and restricted by Donors, 5) Devices are traced during all full lifespan until final recycling, 6) Recycling is restricted to when the use value is lower or there is no demand for reuse, 7) Generate metrics about the circularity of devices.

This has meant making changes to the main eReuse software Devicehub during the first 5 months through a code refactoring that changed underlying technologies like the database.

1) Design and test the tags we need for our use case.

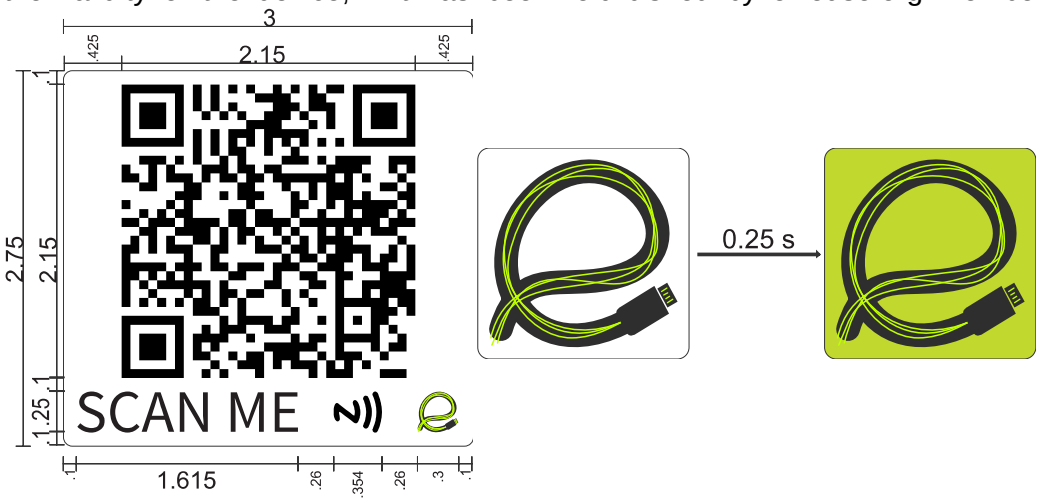
- Resistance (environmental, friction) and data reading tests have been performed on the two sample tags, one photochromic and one NFC. In M3 we received a sample of each. The tags have been hooked onto sample equipment (our personnel) to determine the deterioration. We are currently determining the type of adhesive that best suits metal surfaces, in the middle of the M5 we will carry out these last tests and in the middle of the M6 we will start the pilot with the definitive tag.

- Co-design with TIS partners and eReuse community of the Tags proposal. During M3 and M4 the tags have been defined making up to 5 mockup versions. The document of the final version is inserted as the following sub-section. In the following list we chronologically detail the tag versions and prototypes we developed:

    1. The first proposal includes both the photochromic and the NFC chip in a single tag, alongside a reflective eReuse.org logo. The tag consists of 1) a QR code that regular users can use with their smartphone to get device information, 2) a reflective eReuse.org logo aimed to increase product trust by being difficultly copiable, 3) a written device ID, and 4) a photochromic trash icon thought to be marked when a device is converted from product to waste. This initial design was discarded because the photochromic – NFC manufacturers are different, the a tag with four characteristics would be too expensive, and it would be difficult to ensure end-users or recycling centres mark waste products.

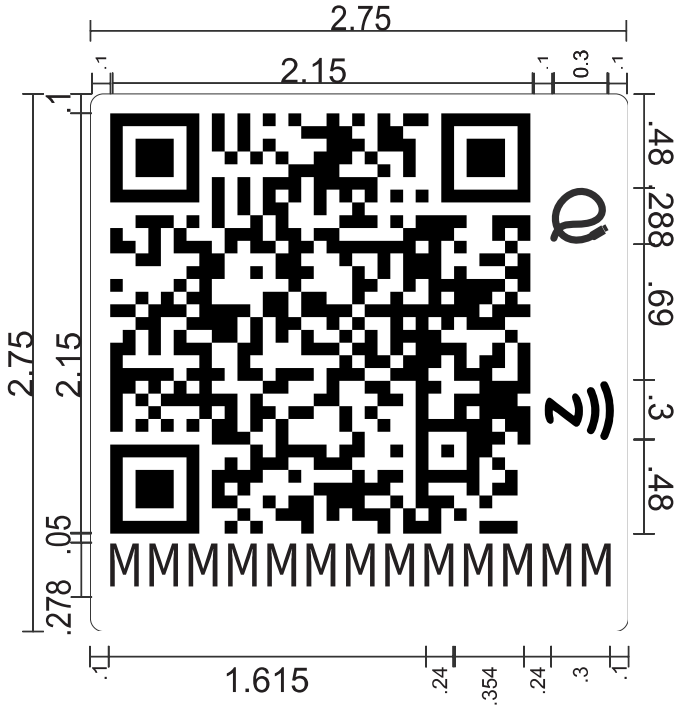
PROPRIETARY RIGHTS STATEMENT
This document contains information, which is proprietary to the TagItSmart! Consortium. Neither this document nor the information contained herein shall be used, duplicated or communicated by any means to any third party, in whole or in parts, except with prior written consent of the TagItSmart! consortium.

2. The second proposal is the first one influenced by the inputs of NFC tag manufacturers. It consists of two tags, one for the NFC manufacturer and another for the photochromic manufacturer. The first tag, the ID tag, consists of a NFC and QR code with texts that shows the tag capabilities. The Photochromic tag has reversible background that changes to green after 0.25 seconds of light and a full eReuse.org logo for validity, and now it is used as a way for an end-user to check the validity of the device; if it has been refurbished by eReuse.org members.

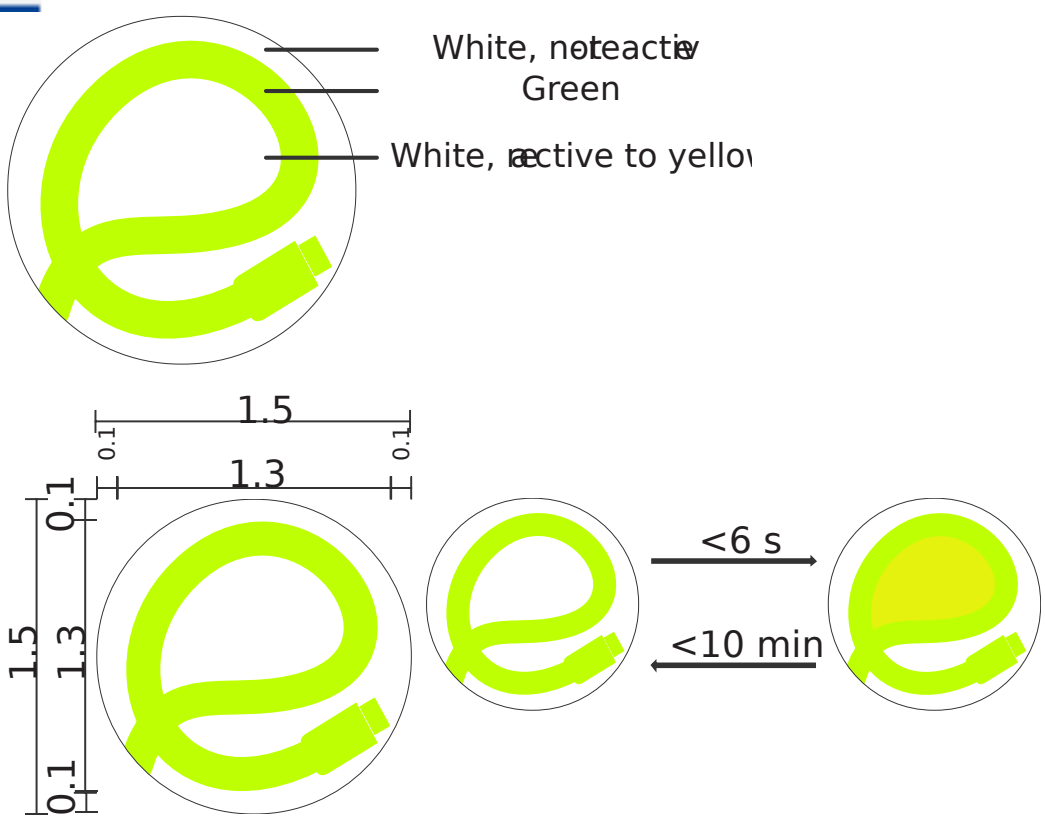


3. After discussions from the NFC manufacturer, the ID tag is re-defined to a third version. The main differences are the values of the QR code, which instead of an ID have a full URL provided by eReuse.org, and the NFC, which have a S/N provided by the manufacturer. The manufacturer in the end could not write the same URL the QR has to the NFC chip, so eReuse.org has to develop a custom technology to be able to operate with both NFC and QR tags. For better usability,

the ID tag gets one part of the QR printed as an ID, and removes colours to keep it all black.



4. After discussions with the photochromic manufacturer, the phtochromic tag is re-designed, being a rounded tag with a white background and a green eReuse.org ‘e’ logo. The interior white background of the ‘e’ reacts by the flashlight of a Smartphone and illuminates for some minutes. The eReuse.org is now only a green colour, a tone of green that differs from the eReuse.org logo but the manufacturer can generate. After testing with the manufacturer, it is agreed that the required minimum time the tag must be illuminated is 6 seconds.



5. After testing several adhesive options the ID tag manufacturer sent to eReuse.org, it is agreed that the NFC tag has a non-marking non-breaking adhesive that adheres to metal and plastic surfaces, making it resilient but easy to remove for the user when refurbishing the device (ex. cleaning it). Below there are videos with the adhesive test performed.

    1. https://nextcloud.pangea.org/index.php/s/vRJXngT1VPU5eLX
    2. https://nextcloud.pangea.org/index.php/s/MvKtsV4IWY49g87

6. The photochromic manufacturer generates and sends the tags during the first quarter of August.

7. The ID tag manufacturer sends at the end of July the final tags, however an error in printing the QR forces the tag manufacturer to re-create and re-send the tags for the second quarter of August.

2) Develop the eReuse.org software modules for compatibility and integration with the TIS modules. The architecture design,

The technical documentation of the tag, including the system design, system usage, and the use-case for ordering tags and introducing them to the eReuse.org systems and Evrything is at the Annex of this deliverable.

- eReuse.org Tag, a server that connects TIS tags with the rest of the eReuse.org software: https://github.com/ereuse/tag
- Modules inside the Devicehub software to manage TIS tags.

3) Develop and test the eReuse.org software modules to implement the SMCG use case.

- Old Devicehub. It requires Python 3.5 and MongoDb 3.4 or newer.
- New Devicehub. It requires Python 3.5 or higher and PostgreSQL 9.6 or higher.
- Teal. Microframework supporting the new Devicehub.

1.4 The final Tag proposal

This section represents the final tag proposal. It is divided in two: 1) the use-case involving the tags, one per type of user, and 2) the design of the tags.

1.4.1 User experience

1.4.1.1 eReuse.org

1. eReuse.org creates a set of empty virtual identities.
2. eReuse.org orders ID Tags from the Tag manufacturer. These tags contain a NFC chip and a QR code stuck on the chip. The QR code represents the ID from step 1. that eReuse.org sent to the Tag manufacturer within the order.
3. The Tag manufacturer sends to eReuse.org the ID Tags with a relationship for each Tag between the ID of the NFC and the ID of the QR.

1.4.1.2 Refurbishers

1. Federated refurbishers have a stack of ID Tags and Photochromic Tags.
2. Refurbishers stick to devices the ID Tag and, by scanning the ID Tag with the eReuse.org Android App, link each tag with the device they are stuck. The eReuse.org system then automatically creates a virtual identity in the Everythng system with traceability information.
3. After successfully refurbishing a device, refurbishers stick the photochromic Tags. The photochromic Tag represents that the device has been successfully refurbished and its chain of custody is tracked by eReuse.org and Everythng.

1.4.1.3 Retailers

1. Retailers pick devices from the facilities of refurbishers and read the ID Tags of the devices to confirm the reception and ensure the device is properly certified.

1.4.1.4 End-users

1. End-users buy second-hand devices from retailers.
2. End-users can apply a more through validation or learn about the life-cycle of the device by reading the ID Tag. For example, the QR code or NFC code scanning app, leads to a Web App with the information about the device.
3. The photochromic Tag provides a quick way for the end-user to validate that the device has been refurbished correctly. The user can apply a challenge to ensure the veracity of the Tag by illuminating it. The Web App, in step 2, allows to illuminate the Tag correctly using the phone flashlight (Android smartphones) or instructs how to illuminate the tag manually in case their smartphone is not compatible (no flashlight for example).

1.4.2 Tag proposal

1.4.2.1 ID Tag (NFC and QR)

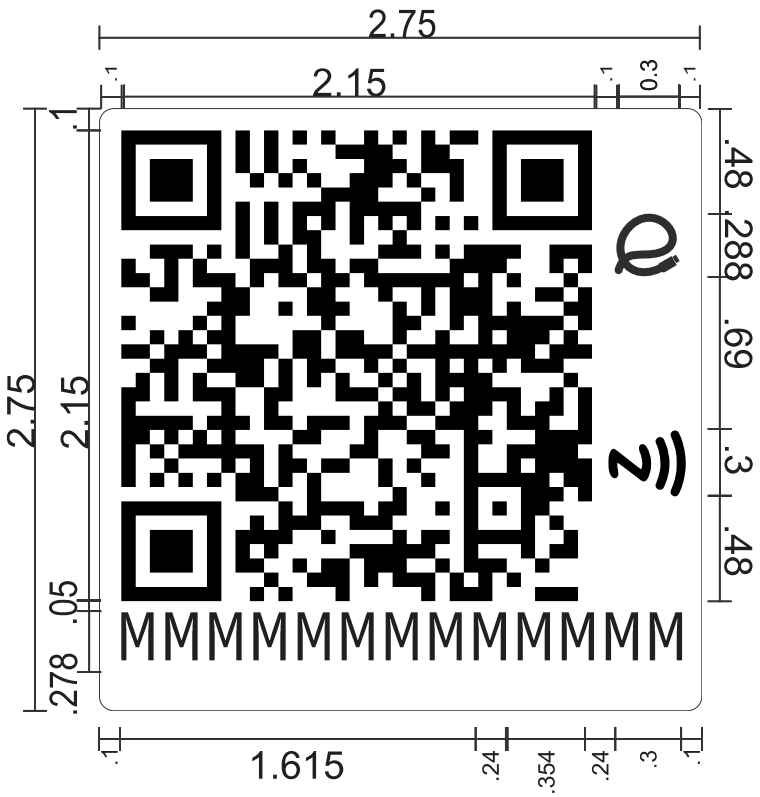
The ID tag identifies the virtual identity of the device. It consists of an NFC Tag with a QR code and the ID value printed on its surface. Refurbishers and retailers primarily use NFC Tags because they are faster and easer to read than QR codes, especially in low-light conditions, while end-users primarily use QR codes due to ease of use.

The ID Tags need to be small so the user does not remove them, specially in small and appealing devices like smartphones, we have to be able to scan the QR code from at least 15 cm in normal office-like light conditions and outdoors; and be able to read the NFC chip from metal surfaces.

The size of the tag is 2.75cm x 2.75cm and it is black-and-white with a white non-transparent background.

The NFC tag contains an ID set by the manufacturer. The QR and printed value contains an ID provided by eReuse.org. For each request, eReuse.org will provide a CSV file with as many IDs as tags to print, and the manufacturer will print an ID to each tag.

The ID provided by eReuse.org is an URL up to 35 alphanumerical characters. The QR code will fully contain the ID, fitting a QR Version 3 with High EEC level (ex. http://t.devicetag.io/MMMMMMMMMMMMM). The printed value will only contain the path of the URL (MMMMMMMMMMMMM), which can be from 8 to 13 characters (from “MMMMMMMM” to “MMMMMMMMMMMMM”); and it will use the open-source font Source Code Pro set at 9.5pt.



1.4.2.2 Photochromic Tag

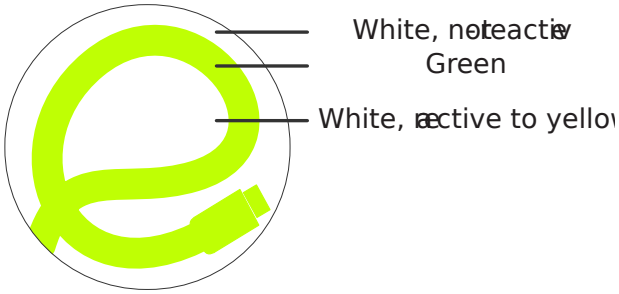
The photochromic **Reversible** Tag helps the end-user to identify a legitimate device that has correctly refurbished by an eReuse.org authorized refurbisher, without the hassle to read the QR code.

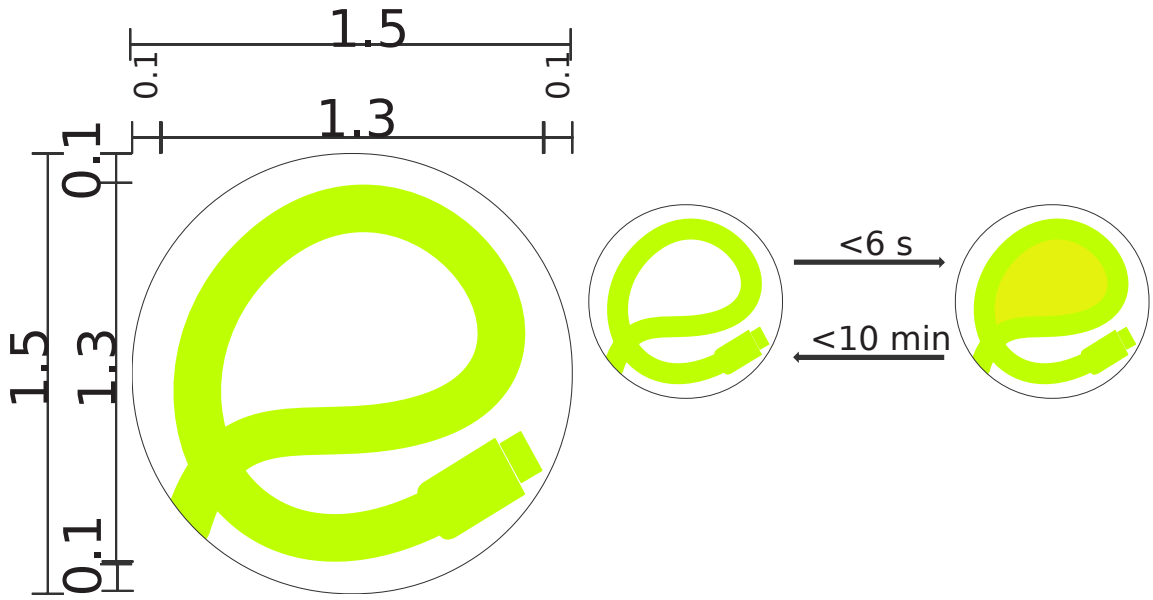
The photochromic Tag has a white background and a green eReuse.org ‘e’ logo. The interior white background of the ‘e’ reacts by the flashlight of a Smartphone and illuminates for some minutes.

In order to being illuminated, the user has to touch the tag with the flash of the smartphone while the flashlight is on for at least five seconds. This leaves a colored mark that slowly disappears, completely fading away in ten minutes.

The ‘e’ color is R / G / B = 191,25 / 255 / 0; CIE La*b* = 92,85; -46,78; 89,37.

The tag cannot easily break while being removed and has to stick in metallic and plastic surfaces, typical for electronic devices.





Section 3 - Conclusions

We have redefined the eReuse.org Workbench and Devicehub to allow for the TIS tags, and use Everythng as the GRD, which results in the architecture that we explained in the section one. Our objective is to fulfil programming this architecture for the end of this project, performing all changes from the existing code. In the case of the Workbench is enhancing functionality that allows linking tags with devices. For the Devicehub is a total re-

development, as the TIS tags is now part of the main characteristics of Devicehub, or the core, at the same time we take the effort in generally improving the software. Finally, we plan to build the GRD on Everythng. Apart from redesigning the architecture, we have started development of the Workbench and Devicehub, focusing on being able to request TIS tags to TIS manufacturers and link them to devices.

Section 4 - References

[1] D1.2 Initial TagItSmart! Reference Architecture and API description [Online]. Available: https://www.tagitsmart.eu/D1.2.pdf

Section 5 - Annex

1.1 Devicehub technical tag specification

The original version of this specification can be accessed at http://devicehub.ereuse.org/tags.html.

Devicehub can generate tags, which are synthetic identifiers that identify a device in an organization. A tag has minimally two fields: the ID and the Registration Number of the organization that generated such ID.

In Devicehub tags are created empty, this is without any device associated, and they are associated or **linked** when they are assigned to a device. In Devicehub you usually use the AndroidApp to link tags and devices.

The organization that created the tag in the Devicehub (which can be impersonating the organization that generated the ID) is called the **tag provider**. This is usual when dealing with other organizations devices.

A device can have many tags but a tag can only be linked to one device. As for the actual implementation, you cannot unlink them.

Devicehub users can design, generate and print tags, manually setting an ID and a tag provider. Note though that these virtual tags don't have to forcefully be printed or have a physical representation (this is not imposed at system level).

1.1.1 eTags

We recognize a special type of tag, the **eReuse.org tags (eTag)**. These are tags defined by eReuse.org and that can be issued only by tag providers that comply with the eReuse.org requisites.

The eTags are designed to empower device exchange between organizations and identification efficiency. They are built with durable plastic and have a QR code, a NFC chip and a written ID.

These tags live in separate databases from Devicehubs, empowered by the eReuse.org Tag software. By using this software, eReuse.org certified tag providers can create and manage the tags, and send them to Devicehubs of their choice.

The section *Use-case with eTags* shows the use-case of these eTags.

1.1.2 Tag ID design

The eTag has a fixed schema for its ID: `XXX-YYYYYYYYYYYYYY`, where:

- *XX* is the **eReuse.org Tag Provider ID (eTagPId)**.

- *YYYYYYYYYYYY* is the ID of the tag in the provider..

The eTagPid identifies an official eReuse.org Tag provider; this ID is managed by eReuse.org in a public repository. eTagPIds are made of 2 capital letters and numbers.

The ID of the tag in the provider (*YYYYYYYYYYYYY*) consists from 5 to 10 capital letters and numbers (registering a maximum of 10^12 tags).

As an example, `FO-A4CZ2` is a tag from the `FO` tag provider and ID `A4CZ2`.

1.1.3 Creating tags

You need to create a tag before linking it to a device. There are two ways of creating a tag:

- By performing `POST /tags?ids=...` and passing a list of tag IDs to create. All users can create tags this method, however they cannot create eTags. Get more info at the endpoint docs.
- By executing in a terminal `flask create-tags <ids>` and passing a list of IDs to create. Only an admin is supposed to use this method, which allows them to create eTags. Get more info with `flask create-tags --help`.

Note that tags cannot have a slash `/`.

1.1.4 Linking a tag

Linking a tag is joining the tag with the device.

In Devicehub this process is done when performing a Snapshot (POST Snapshot), by setting tag ids in `snapshot['device']['tags']`. Future implementation will allow setting to the organization to ensure tags are inequivocally correct.

Note that tags must exist in the database prior this.

You can only link once, and consecutive Snapshots that have the same tag will validate that the link is correct –so it is good praxis to try to always provide the tag when performing a Snapshot. Tags help too in finding devices when these don't generate a `HID`. Find more in the `Snapshot` docs.

1.1.5 Getting a device through its tag

When performing `GET /tags/<tag-id>/device` you will get directly the device of such tag, as long as there are not two tags with the same tag-id. In such case you should use `GET /tags/<ngo>/<tag-id>/device` to unequivocally get the correct device (feature to develop).

1.1.6 Tags and migrations

Tags travel with the devices they are linked when migrating them. Future implementations can parameterize this.

1.1.7 Use-case with eTags

We explain the use-case of tagging a device with eTags, going through the manufacturing of the tags, their distribution and the final linkage between tag and computer.

For this exemplifying use-case we assume we want 100 eTags.

1.1.7.1 Actors

- Tag provider: organization that orders and manages the eTags; it is certified by eReuse.org thus having permission to order the tags.
- NFC Tag manufacturer.

- Photochromic tag manufacturer.
- User: organization that uses the tags.

1.1.7.2 Requirements

- At least one eReuse.org Devicehub. One Devicehub can contain several organizations and inventories, or organizations can have their own copy of Devicehub. Devicehub work distributely over the Internet.
- One eReuse.org Tag software running in a server over the Internet by the *tag provider*.

1.1.7.3 Use case

1. The *tag provider* enters into the server containing the *eReuse.org Tag* software and executes the command `etag create-tags 100 --csv file.csv`, which creates 100 tags in the database and saves their URLs into a spreadsheet CSV file called *file.csv*.
2. The *tag provider* sends the CSV file to the *NFC tag manufacturer* and orders the 100 tags.
3. The *NFC tag manufacturer* creates those tags (NFC plus QR code) and updates the CSV file with the NFC ID of each tag, so each row of the CSV file contains the URL sent by the *tag provider* and the ID of the NFC tag created by the *NFC tag manufacturer*.
4. The *Tag provider* updates *eReuse.org Tag* with the ID of the NFC by executing `etag update-tags file.csv` where *file.csv* is the file sent by the *NFC tag manufacturer*.
5. The *Tag provider* orders 100 photochromic tags to the *Photochromic tag manufacturer*. Note that these tags don't require any special treatment.
6. The *Photochromic tag manufacturer* sends back 100 tags.
7. The *Tag provider* distributes the eTags (NFC and photochromic) to several organizations, *users*, both physically by sending them and virtually by executing `etag set-tags http://some-devicehub.com 0 100`; this marks the tags in *eReuse.org Tag* as *sent to some-devicehub.com* and creates the tags in that Devicehub.
8. The *user* receives the tags, sticks them in their devices, and scans the NFC or QR codes:
    1. By using the eReuse.org Android App the user can scan the QR code or the NFC of the eTag.
    2. If the *user* is processing devices with the eReuse.org Workbench, Workbench automatically attaches hardware information like serial numbers, otherwise the *user* can add that information through the app.
    3. These softwares communicate with the Devicehub of the user and command the Devicehub to link the device with the tag.
    4. The Devicehub of the user links the tag.
    5. The Devicehub creates or updates a virtual entity in Everythng containing the device and the tag.
    6. If Devicehub or Everythng detect that the tag was linked they won't allow this operation. Devicehub can only detect if the app is linked by looking at its internal database. Everythng, as it contains all device and tag information, validates that the tag is not linked elsewhere.