Scaling the Verifiable Digital Product Passport

Summary

Attaching a Digital Product Passport to goods is made mandatory by law in the combined context of reducing climate externalities and fulfilling CSR requirements. Purely informational DPPs first apply to product items considered as equivalent. The traceability of states and ownership however requires to uniquely and permanently identify any single item in a product line or even occurring as a component to a bigger system.

Finding the proper ways to globally achieve such per unit auditable and secure traceability is a challenge, specifically when blockchain technology is considered.

The article shows how the KeeeX technology can be leveraged to address the Digital Product Passport in all its flavors, from generic product-based customer information to per item serialized codes allowing for the traceability of maintenance, recycling, decommissioning and proof of ownership to enable a second market.

Author: KeeeX, Laurent Henocque, contact@keeex.net, https://keeex.me

1. Introduction

The Digital Product Passport (DPP) is a digital sheet that provides information on a product's origin, composition, repair and disassembly options, and how individual components can be recycled.

It enables stakeholders throughout the value chain (producers, importers, distributors, repairers, recyclers, consumers, etc.) to share and access this data more easily.

The digital product passport will be required for all products covered by the European "Ecodesign for Sustainable Products Regulation" (ESPR).

The objectives of the digital product passport are to:

- Kick-start the transition to sustainable consumer products towards a more circular economy.
- Enable companies to share product data to facilitate reparability, reuse and recycling.

- Inform consumers about the environmental impact of products and give them the means to adapt their purchasing behavior.
- Meet regulatory requirements on product eco-design.

2. The situation

Most products sold today provide little or no information regarding their conditions of production and recycling options. Most products sold today provide instructions in the form of a paper leaflet or book that uselessly destroys trees and is barely ever available when a repair or end of life condition occurs, several years after the acquisition.

The GTIN number (GS1) could be used to retrieve product data but fails to inform about where to fetch this information from since it does not precisely direct the user to a place that exposes details.

The GS1 "augmented" QR Code instead provides a "resolver" URL (the "Digital Link") to retrieve the product DataSheet and potentially more information, including data relative to batch and/or serial numbers. When present, this information enables the digital link resolver to provide further information and services.

3. Challenges

The requirement to address reparability and recyclability also entails to account for the transfer of ownership or responsibility of a product and/or its parts. Of course, such transfers also occur along the supply chain and retail processes, with a product ending in a customer's hands, then later entering a second market, repair, recycling or destruction.

The goal of also tracing impact over the entire life cycle moreover requires addressing the supply chain aspects of boxing / unboxing and binding the item to the information relative to container transfers, vessel / plane / truck emissions and so on. The measure of impact is also increasingly becoming a legal and tax requirement.

The aim of fighting counterfeiting or grey markets requires the existence of dedicated (if not global) and if possible trustless registries.

No public blockchain solution today exhibits the capacity required to handle the total volume of all individual items produced worldwide.

4. Quick intro to KeeeX

A perfect entry point of knowledge on KeeeX can be found at KeeeX's website: https://keeex.me

The KeeeX offer combines a full software suite combining off the shelf apps, components and apis that cover Data protection and Traceability in general to the extent of implementing the MLETR and Data Lineage prerequisites:

- **KeeeX Fusion** is a backend software component used to keeex, sign, verify files on premises
- **KeeeX Vault** is a wallet delivering private keys under absolute user control
- **KeeeX JS** is a library allowing for "in app" / "in browser" verifying, keeexing, signing files using KeeeX Vault keys.
- **KeeeX Chain** is a Geth based publicly auditable hybrid EVM blockchain operated in layer 2 of Bitcoin
- **KeeeX Stories** is an API and service for historizing sequences of events, data and documents. This addresses issues that "blockchain" does not handle well. KeeeX Stories operates in layer 2 of both Bitcoin and KeeeX Chain.
- **KaaaS** (https://kaaas.keeex.me) is a web portal for creating and signing dropped files or in portal created documents
- **KeeeX Collect and Prove** is a mobile app for digitizing field processes and gathering verifiable probative field data, photos and videos
- **KeeeX API** is a web service and solution combining timestamping and mutualized Bitcoin anchoring

KeeeX addresses trust issues with the help of several levels of trust:

- **Unforgeable embedded proofs inside documents** and files. Files hold a permanent record of their authors, integrity, and bindings to blockchain registries
- **Unforgeable sequences of chained metadata files** relative to privately held events, data and documents that pertain to a process.
- **Unforgeable embedded links to smart contracts** within files that allow for attaching mutable (yet unforgeable and auditable) properties to immutable Data and files
- **Smart contracts** operated by default on KeeeX Chain, possibly on any (even non EVM compatible) blockchain or private registry
- **Multiple daily anchoring certificates on the Bitcoin blockchain** (CO2e emissions are compensated). Each certificate receives a qualified RFC3161 timestamp. Each file may download the full certificate of their own bookkeeping or request their merkle branch in the rollup for embedding and thus permanent tierless verification.
- **Per file RFC3161 timestamps**

Figure 1 summarizes the contents of a keeexed file

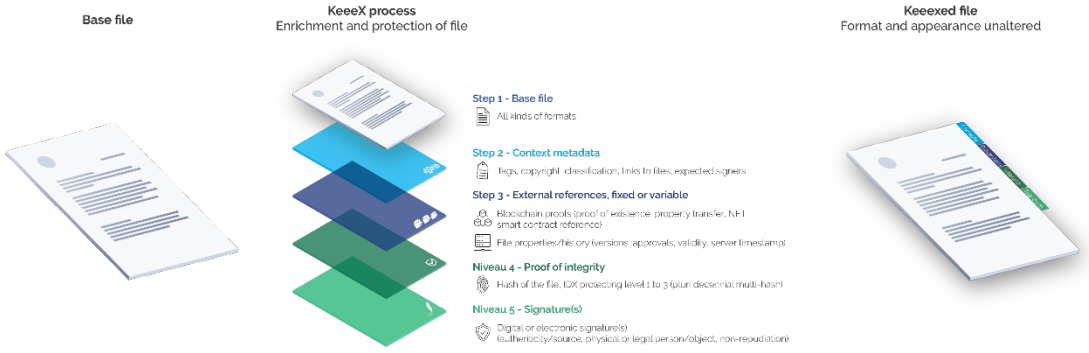

Figure 1 The KeeeX embedded metadata layers

At the file level, our technology embeds four metadata layers within files: technical (as per user intent), external references to other files and smart contracts describing variable properties or versions, a multihash with lasting properties, and multiple signatures supporting delegation according to predefined roles and endorser. This can be complemented with embedded RFC3161 timestamps and embedded Merkle proofs of Bitcoin anchoring for absolute tierless verification.

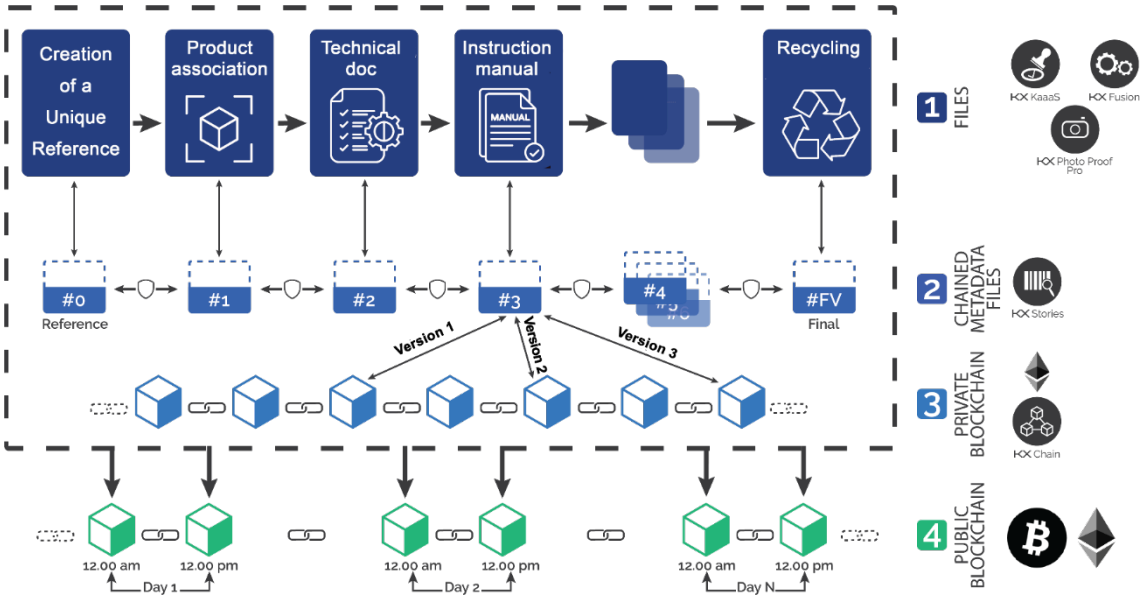

Figure 2 The KeeeX layer 2 blockchain infrastructure

At the process and dynamic level as described in Figure 2, our offer leaves the files by their owners, and delivers an historization mechanism implemented using chained metadata files (through the KeeeX Stories api) mapping to the actual files under access control set by the file owners, in layer two of our publicly auditable EVM hybrid blockchain KeeeX Chain, itself as well as all other files in layer 2 of the public Bitcoin blockchain for outstanding durability of proofs (embedded as Merkle branches as explained above).

5. How KeeeX handles DPP issues

Per product Digital Product Passport

The first goal of the DPP is to provide the user/customer with accurate and if possibly verifiable information about:

- General information about the company, mission, objectives, ethics…
- The constituents of an item at hand
- How it was produced, including CSR and climate Impact
- How to repair, recycle, delete
- Where to trade as second hand if desirable

- …

GTIN - GEPIR - the state before

GS1's GTIN[1] combines in a single code a company and a product prefix. Every product is registered with attached information. GS1 provides a service that can be publicly queried to display some of the product information.

Using standard GTIN, the GS1 "GEPIR" portal https://gepir.gs1.org/index.php/search-by-gtin allows for retrieving brand and product information as they are known from GS1. Test for instance using 8714574662879.

GTIN - Verified by GS1 - the state now

As of dec. 30 2023, the above system is replaced with the "Verified by GS1" service: https://www.gs1.org/services/verified-by-gs1/, for instance to be tested with 2043338000012 (go there using https://www.gs1.org/services/verified-by-gs1/results?gtin=9506000140445#productInformation)

It must be noted that beyond textual information, nothing close to a digitally signed commitment by the brand occurs there. The portal is entirely under the control of GS1 that acts as a central trusted tier here.

> *KeeeX enables brands to create verifiable documents that may be saved on the side by a customer while retaining their verifiability. This may serve several purposes, including creating a folder with digital maintenance sheets for all one's belongings, retain for accounting of tax purposes (in view of scope 3 carbon emissions for instance), retain for proofs of good practices in CSR context…*

Of importance too is that almost nobody except professionals knows or cares about the GEPIR and Verified by GS1 portals.

Digital links - the future

The digital link involves a resolver url, that when traversed gives access to the information that the brand wishes to share with their customer, from the above list and more.

In contrast with what precedes, the url can be followed by simply flashing a QR Code, which is far easier than querying a portal with a text to type (even though the portal might offer the service of flashing the barcode).

In contrast too, the brand now may suffer impersonation attacks, with fake products linking to perfectly forged phishing resolver urls.

[1] Full documentation access from GS1 websites as https://gs1.fr … Also check the references section at the end of this document

A/ Using QR Code based digital links, the brand is free and responsible to deliver their information to their customer. In order to protect their reputation and customers against fake information that might accompany a counterfeit, they have the possibilities to:

- Issue verifiable documents on their portal
- Expose a file verifier on their main website, protected by their TLS/HTTS certificate

> *KeeeX is designed to produce such standalone verifiable documents, that embed one or several digital signatures that no counterfeiter can copy. Our customers also deploy a verifier on their website, protected behind TLS/SSL https access, that can inform when a file was not issued by them even if valid in terms of keeexing. Check https://www.enedis.fr/medias/verificateur for instance.*

B/ It may occur that between the time a product was sold (and the customer first accessed product information and possibly saved their copy of some documents critical to them like those concerning repair, warranty, spare parts…) and the moment when the document becomes useful, it has changed version.

> *KeeeX provides a one of a kind patented solution that enables the brand to declare within any file the smart contract or registry access that tracks such changes and directs to the latest version of some documentation.*

C/ Providing url resolvers via package/item datalinks opens the way for phishing attacks, where a counterfeiting company would create packages exposing a misleading url. It is of importance that instead of giving direct content access, the resolver url returns an unforgeable file holding verifiable digital signatures and asking for their verification, therefore delegating access to content.

> *Again, KeeeX enables the production of such a proxy document.*

D/ A desirable property is that the Digital Link provides at least partial verifiability against the file exposed by the resolver. This is possible since that after the core standardized part of the url and starting at the question mark, free content is available.

> *We recommend deriving a complementary product code from the received file's IDX. The IDX being a cryptographic hash of minimum 256 bits, it is statistically unique at universe scale. By extracting a limited number of the first characters in this code, we obtain codes that may be unique corporate wide, even though they would globally expose harmless redundancies.*
>
> *For instance, the product code may be constructed from the first N characters of the IDX's encoding, followed by an integer in case of redundancies.*

Example: considering the IDX in readable form "`xopod-runak-nefat-ceduh-cumis-hybyh-maluv-goten-symuv…`"(17 words total), a derived code might be "`xopodrunak00`" (then '`…01`' etc. in case of conflicts). Using the more effective encoding B58 yields shorter more precise codes: "`GdXHBfhFUKtYjuJXmaxWUEZ2eVxB2qxVCDVLkDeVNmT8`". An eight-digit extract

"GdXHBfhF" allows for deriving the family of 10-digit codes "GdXHBfhF" then "GdXHBfhF1"…

When the file is downloaded, its IDX can be checked against the short extract used as a code, which provides an early level of tierless bidirectional verifiability.

If case full client-side or server-side verifiability is needed, or when the IDX is used as a search entry on the server, the full IDX can be used in the shortest available web compatible encoding (B58 is designed for the purpose).

GS1 Digital Link specifications require using at least a GTIN key in the resolver URI. More detailed information can be provided in extra parameters. Since the GTIN combines corporate and product IDs the retrieved file can be verified for integrity and origin, and the contents matched with the product id present in the GTIN.

Shortened hash example

https://gs1.keeex.it/01/2043338000012?idx=xevan-budod-sezam

Full length hash example

https://gs1.keeex.it/01/2043338000012?idx=xevan-budod-sezam-zeruv-lukyn-pamyh-pidop-volum-zokef-vukip-futut-levic-lihef-vokez-zamad-nakih-zyxax

The two above examples illustrate how adding the expected idx (or maybe just part of it since collisions are seldom) enables the tool used to resolve the digital link to assess the match between the expected idx and the one that can be obtained by verifying the file on a keeex verifier, like https://s.keeex.me/verify.

In theory providing the idx parameter would suffice to any subsequent interaction based upon the retrieved and verified file contents. This complements the cybersecurity of the digital signature present in the file that an attacker cannot fake and makes adding a signature to the qrcode mostly useless.

E/ Automation is possible since Digital Product Passports may unlimited amounts of automatically generated and automatically processed technical Data. Support for achieving the dual service of visually elegant presentation for human users combined with easy automation for processes is provided by combinations of XSL/XML, HTML/JSON etc.

Per batch Digital Product Passport

Products may be produced by batches, where such batches may slightly differ in their characteristics or components (in ways that to not require emitting a new product code). The Digital Link acknowledges this by enabling to mention a batch number on individual items (often alongside useful expiry dates). This can be verified by anyone by looking at a box of medication for instance.

Within the GS1 framework, Batch numbering requires no declaration and is the responsibility of the corporation.

Since Batch information is passed to the resolver url in the Digital Link, the resolver may present the user with accurate specific batch details in complement to more global Corporate or Product information.

Here again, the batch specific data must be presented to the user in a form that they can retain for their own use, and that can provably be bound to the batch itself by a digitally signed commitment.

> *KeeeX enables all batch related Data to be digitally signed by (an authority) in the Brand and/or Product line and be made verifiable with no time limit and no business model.*

Again, there may exist the need that documentation points to smart contracts or registries tracking special events, like when a car company must launch a campaign to return its vehicles due to an anomaly.

> *KeeeX enables the brand to declare within any verifiable file the smart contract or registry access that tracks such information, thereby maximizing the chance that a user gets informed.*

Batch numbers often occur in linear series. This is not always wanted for confidentiality or anti-counterfeiting reasons. Batch numbers can be made technically unique as the result of making them the result of keeexing a self-verifiable file. The usefulness of this will be better understood with unique serialized item codes.

Shortened hash example:

GS1 Digital link provisions key 10 for declaring a batch number. Again, a specific key can be used to denote the data file that is expected as a return

https://gs1.keeex.it/01/2043338000012/10/ABCD?idx=xesag-lylum-zyhyr

Indeed, the file retrieved for a batch will include a verifiable reference to product information, in a "complement or replace" mode. No link to product level data must then be provided in the QR Code.

Per item DPP leverage unique serialized Item codes

Serialized item codes are a tool of choice to perform unit tracking: change of owner/caretaker, maintenance/repair/destruction status, impact specifics relative to eCO2 emissions or CSR (supply chain mode of transport). They also enable efficient anti-counterfeiting and anti grey market resale.

One challenge is that no blockchain solution can scale to the metrics of the global supply chain / retail economy. For instance, 100 to 150 billion textile items are sold yearly worldwide.

Anti-counterfeiting

We address the subject of counterfeited items to be sold within the regular retail circuit, in contrast with deliberate fakes sold on ultra-cheap circuits.

Provided that they occur in a non-linear series, serialized codes cannot be guessed by a counterfeiter. If we assume the existence of a registry capable of telling which codes are legit from the ones that are not, the only possibility left for a counterfeiter would be to replicate one valid code (or even a few different ones but this does not change much).

As said above, blockchain is as of today most probably not suited for the declaration of every single tradable item. But there is good news as this is not mandatory.

> *Every serialized item can be identified using a description file as detailed above. Such a file contains a verifiable reference to the matching product and/or batch description file, technically exploited with complement or override semantics.*
>
> *Being keeexed, the file contains one or several legitimate signatures by the production authorities (whether at corporate or product line level). No counterfeiter can reproduce this as long as a signing private key was not leaked. Valid signing public keys can be publicly announced on the corporate web site via an api behind TLS/HTTPS security. They may also be registered and advertised using a specialized smart contract designated within the file.*
>
> *To achieve the volumes anticipated in the global retail economy, these keeexed files are anchored on the Bitcoin blockchain, plus if available on a smart contract blockchain operated at corporate level. Blockchain anchors are mutualized, which yields extremely limited impact (150 tons eCO2/year for KeeeX, fully compensated within our entire company's emissions).*
>
> *The main point is that* ***it is not required that every single retail item is registered in a public blockchain smart contract using its identifier as a token ID****.*

Invalidated codes

Production lines generate not for resale items because of errors or incidents. The matching codes must be invalidated.

Alternatively, the fact that a code is flashed in different incompatible situations raises the alert that some counterfeiting process is at play.

In both cases the brand is fully motivated in handling the case properly. This means that when receiving a serial code with a problem via digital link dereferencing, they will inform the user by a means or another.

> *However, making the information global may require writing within a dedicated smart contract. This smart contract is referenced within the item data file.*

Adding a smart contract for telling whether a code was invalidated or has achieved a certain level in the distribution process is enough to prevent any actor attempting to scale a counterfeiting business: when the same code is encountered for a second time, this signals the existence of a fake. Any actor holding the first item may be warned that he is potentially in presence of a fake.

> *The volumes of such declarations is compatible with scaling.*

Other properties

Change of ownership, as well as all issues regarding the status of an item along its life cycle can be traced using a smart contract. Such smart contracts can be operated on any blockchain and are unforgeably referenced within the keeexed item data file. Since the smart contract uses the file's IDX as a tokenID, a provably unforgeable bi-directional link is created between the item data file and the blockchain. Different smart contracts can be used for a same product if needed.

> *KeeeX leverages an ERC721 smart contract on KeeeX Chain to implement ownership actions, although our users are free to pick any smart contract on any blockchain for this (even non ETH based, and even non EVM compatible)*

Shortened hash example:

GS1 Digital link provisions key 21 for declaring a serial number. Again, a specific key can be used to denote/partially control the data file that is expected as a return.

Example Digital link

https://gs1.keeex.it/01/2043338000012/10/ABCD/21/1111?idx=xucez-ryvid-putel

6. About change of ownership, repair, recycle and destruction

The context of change of ownership or responsibility applied to an individual item requires a unique serial code. This serial code may be attached to the item from inception, or

opportunistically created when it becomes necessary to bind unit related properties, events or data.

When the serial code is defined from inception it can be attached to the item itself or to some packaging and delivered through a QR Code or an RFID device exposing their serial UUID.

The serial code is the binding glue between the physical item and the digital content that accompanies it, be it purely informative (how to repair), operative (who is the owner, repair history, destruction status) or even acting as a digital twin (3D view of components and their history).

Beyond serialized codes, all of change of ownership, repair, recycle and destruction situations also require signing capability by actors. Every such action will apply to the serial code and will be signed by some authority: the owner, the repairer, the retailer placing the refurbished item or part on the market, the destruction company.

Only the owner can sign a change of owner action.

> *Ownership is thus modelled using public key cryptography exactly like in a cryptocurrency context. Recycle and destruction actions also require the transfer of ownership and thus require leveraging a signing capability. In repair actions, the repairer commits to their own responsibility and should as well digitally sign their actions.*

Exclusive control requirement

Since the DPP must trace the ownership and caretaking responsibility of goods, it acts as a digital twin for the physical item. Proving that ownership changed must be acknowledged by a registry. Modern cryptography and the blockchain space suggest that such a registry should ideally be implemented by a smart contract on a blockchain. In some instances, registries may be provided by a trusted tier (for instance operated by a governmental or regulatory body). The registry should replicate possession of the physical item by exclusive control. This requires to:

- identify the person having exclusive control;
- make sure it is the only one to have control and be able to transfer it;
- ensure that it loses full control when the transfer takes place, and finally;
- ensure that it cannot exercise the right or its transfer more than once.

Finally, we need to be able to trace everything reliably.

Exclusive control of a digital asset has been an integral part of the foundations of blockchains since 2009, first in a monetary context (Bitcoin) and then in a technical context (Ethereum smart contracts).

Blockchain technology cannot be ignored

Blockchain is the only potentially publicly auditable (or in this case "traceable") tool capable of guaranteeing the exclusive control of a serialized DPP by exercising the ability to produce the digital signature of a transfer transaction or of the exercise of an action. The case of change of ownership is exemplary, as it has been used in real life in the world of crypto assets since 2009 by the Bitcoin protocol (transfer of ownership of digital units of account) and more recently and more visually by NFT initially on the Ethereum blockchain (transfer of ownership of Non-Fungible Token identifiers).

More generally, the DPP context suggests the public traceability of other serial code attributes such as the status (retail, first hand, second hand, recycled, destroyed), as well as attributes bound to some verifiable documentation: most recent version of repair/recycle/destroy instructions for instance. Here again, electronic registry technology enables the traceability of changes in the values of variable properties attached to a document, under all the required constraints (author of the modification, prohibited modifications, etc.).

However, the context of dematerialization of DPP history is not that of public blockchains: there is no question of fighting censorship, and decentralization of writing (which most of the time remains an empty word) is therefore unnecessary. On the contrary, the industry needs scalability and access control for writing system status changes, while guaranteeing their absolute opposability, and in some cases their pseudonymity, through the effect of a digital signature effectively under the exclusive control of their issuer.

Blockchains have also given rise to the development of a huge number of signature tools under the exclusive control of users: software (Metamask, ZenGo...), physical (Ledger Wallet, Trezor...) and among the latter so-called "air gapped" systems (Ellipal...) requiring no connection between the signature device and the host software through the use of communication verifiable by QR codes.

In many cases, exercising the ability to sign a transfer transaction to the recipient's digital identity perfectly reproduces the hand-to-hand transfer of a physical good bound to their Digital Passport. Instead of a handwritten signature of receipt, the recipient's ability to digitally sign a future action using the digital identity designated by the previous owner materializes exclusive control.

More precisely, if we take up the above formulation of exclusive control requirements, we observe in the blockchain universe that:

- the ability to sign with the private key corresponding to an expected public key identifies the person with exclusive control;
- an appropriate smart contract guarantees that only this person is able to initiate a transfer;
- the same smart contract guarantees that once a transfer has been made, the person cannot repeat it;
- the blockchain protocol guarantees that no two simultaneous transfers are possible (on the same network).

KeeeX operates an official release GETH based hybrid blockchain called KeeeX Chain.

No one should be able to create a false document or issue a false transaction.

First of all, we strongly believe that:

- No one can agree to interact with dematerialized documents entitling them to goods of arbitrary value (as in the case of the Bill of Lading) without the highest guarantee that no one will be able to cheat;
- There is no middle ground for the notion of *exclusive* control.

In the context of the serialized DPP allowing for transfer of ownership or responsibility, these requirements recommend ruling out any digital signature produced using a private signature key accessible to third parties[2], unless the user is provided with the necessary warnings or information on the limits of insurable value. This is all the more so in the case of interactions that only weakly identify a user (even if only by sending an e-mail or SMS), provisions that are nonetheless valid in the context of qualified electronic signatures.

A DPP requiring a signature interaction (digital or electronic) can therefore only be signed by an identity that has exclusive control over its means of signature, whether by a software device used in a portal or application ("software wallet"), or by a physical device ("hardware wallet"). It should be noted that this condition does not preclude a DPP or document process from authorizing several actors (presumably from the same company) to work on the same DPP process, notably for backup purposes (risk of loss of means of signature), in a context where the traceability of signatures and signatories is enforceable.

> *KeeeX tools leverages a self custody wallet solution called KeeeX Vault together with the KeeeX JS web SDK, allowing users to decipher a private key within a portal or mobile app to create digital signatures under their absolute control.*

A few years ago, this requirement might have seemed excessive, but the accelerating democratization of signature methods in the world of crypto-currencies and blockchains, as well as the forthcoming eIDAS2 regulation and Estonia's experience, make it perfectly conceivable. Indeed, no one would object to the use of what looks like a Fido key or equivalent, already widespread as second-factor authentication tools.

Documents to be guaranteed are not just PDFs

The documents and data involved in a dematerialized process around transferable items and documents are extremely variable. This is true both for the serialized DPP themselves, which are the subject of the transfer, and for the appendices that support the decision-making process. Of course, there are image files, html files, csv files, json files, excel and

[2] This is notably the case for a signature produced by an RGS** type physical device, whose unlocking password is accessible on a back end in a cloud-type remote interaction.

other files, office files (e.g. Word), which are invaluable for tracking changes, etc. (and yes, they can also be pdf files - but why have to produce them if they can be avoided).

> *The KeeeX Fusion solution processes any file format, then involved in any possible KeeeX Story historization chain.*

Verifiability

Data, documents, sequences and proofs must be easily verifiable by anyone, anywhere, without time limits or business models. In particular, any element of a dematerialized process must be verifiable without the need for a third party to create an account or make a payment. This verifiability is closely linked to the notion of reliability: the more verifiable a solution, the easier it is to demonstrate its reliability.

In this context, any solution that gives the illusion of security through a complex device is inferior to one that provides easy access to verification. In the paper world, this is evidenced by the very poor ability to verify watermarks or filigrees (as in the case of Bills of Lading on special paper or banknotes) or holograms (banknotes in general), and in the electronic world by the general inability to verify PDF signatures.

Several conditions must be reliably verifiable in order for the holder of a DPP and relevant documentation to have the same rights as a physical security:

- Contents
- Its original character
- Identification of its holder and signatories
- Its integrity
- Its date
- Its evolution

Finally, in certain contexts, the verifiability of a part of the document must be possible without revealing the entire document: for instance, to disclose the declaration of the absence of hazardous materials without exposing the full list of components of the goods. This is made possible by technical tools widely used and tested in the blockchain world, including "Zero Knowledge Proofs" and "Merkle branches".

7. RFID

QR codes are one cheap way to bind identifiers to product items. QRCodes however do not guarantee that flashing them occurs in presence of the item, since the code may be sent digitally.

Even though QRCodes have been shown to address mass counterfeiting by essentially forbidding to manufacture large series of fakes, recent RFIDs that involve various levels of cryptography provide several interesting features:

- Scanning an NFC is "provably" made at a very close distance of the tag (a few centimeters)
- Reproducing an NFC is impossible if the device encapsulates a secret key (used for AES cryptography) or even better if the NFC provides digital signature capability.
- Substituting an NFC can be made impossible since inlay makers have made outstanding progress at embedding RFID devices into various materials, ranging from glass to concrete or leather.
- Some NFCs can digitally sign a challenge provided by the requestor, thus enabling the NFC to prove that it has seen the requestor

All strengths combined allow for proving that an NFC scan was actually made in the presence of the actual item it pertains to (when the NFC exhibits digital signature capability, so as to ensure that no insider can counterfeit an interaction). Assuming that the RFID device can itself be provably un copy-able, RFID thus enables anti-counterfeiting at the first occurrence

RFID tags an expose a URL in the same way as a QR Code does and can thus be tuned to address the same issues as was previously explained. They however possibly additionally deliver a wealth of extra services: for instance, by providing captor measures allowing for tracing temperatures, battery levels etc.

It should also be mentioned that scanning NFC tags provides a better experience that QRCodes (taking the locked phone next to the object suffices to trigger an action) and also that NFC tags can be embedded (in leather, concrete, glass etc…) and thus be made scratch and time resistant.

8. Conclusion

The article shows how the KeeeX technology can be leveraged to address the Verifiable Digital Product Passport at scale in all its flavors, from generic product-based information made available to customers to serialized per item codes allowing for the traceability of maintenance, recycling, decommissioning.

9. References

https://keeex.me

https://environment.ec.europa.eu/strategy/circular-economy-action-plan_en

https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1583933814386&uri=COM:2020:98:FIN

https://commission.europa.eu/energy-climate-change-environment/standards-tools-and-labels/products-labelling-rules-and-requirements/sustainable-products/ecodesign-sustainable-products-regulation_en

https://commission.europa.eu/energy-climate-change-environment/standards-tools-and-labels/products-labelling-rules-and-requirements/sustainable-products/about-sustainable-products_en

https://environment.ec.europa.eu/publications/proposal-ecodesign-sustainable-products-regulation_en

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022DC0140&qid=1649112555090

https://www.gs1.fr/qr-code-augmente-gs1

https://www.gs1.fr/gs1-digital-link