Disposable Yet Official Identities (DYOI) for Privacy-Preserving System Design

The case of COVID-19 digital document verification and credential-based access control in ad hoc outdoor and indoor settings (and beyond)

Paper to be presented at Data for Policy 2020 Conference
https://dataforpolicy.org/data-for-policy-2020/

Petros Kavassalis[1], Nikos Triantafyllou[1], Panagiotis Georgakopoulos[2], Antonis Stasis[1], Rob van Kranenburg[3]

1: University of the Aegean | 4m Lab
2: Athens University of Economics and Business
3: #IoT Council, Resonance Design BV

Corresponding author: Petros Kavassalis < pkavassalis@atlantis-group.gr>

Draft Paper[1]
Document History
V2.1: 28.04.2020
V2.11 04.05.2020
V2.2 19/05/2020
V3.0 02/09/2020

University of the Aegean - School of Engineering
UAegean | i4m Lab

[1] This research has received partial funding from the European Commission (SEAL project funded by CEF under Grant Agreement No INEA/CEF/ICT/A2018/1633170) and from SIEMENS (SBchain project funded via Settlement Agreement with Hellenic Republic).

Table Of Contents

0. Introduction and Summary

"We cannot solve a pandemic by coding the perfect app", as a recent Electronic Frontier Foundation (EFF) paper meaningfully suggests[2]. However, as several countries around the world currently take action to prevent and prepare for the second wave of COVID-19 pandemic, the use of COVID-19 tracking applications is a centerpiece of the policies in the upcoming months[3]. A relatively recent report of the French Inserm (EPIcx lab)[4] postulates that the effectiveness of the different, possible lockdown exit strategies depends on their capacity to control the epidemic in the new conditions of moderate social isolation and reduced mixing of populations[5], which is a two-fold requirement. On one hand, social distance measures should be actively maintained and on the other hand, aggressive testing should be conducted to promptly identify infectious individuals and isolate them. Yet, such a systematic and large-scale testing should be combined with promptly executed (by definition) and widespread digital contact tracing (i.e., adopted by a large part of the population), in order to be really efficient (since manual testing is really slow and cannot be scaled up)[6].

The current approach for digital contact tracing adopts a clear "mobile-first" perspective and uses "proximity tracing[7] technology which measures Bluetooth signal strength to determine whether two smartphones are close enough, without however revealing the real identity of the contacted people (because of the use of rotating or Ephemeral IDs[8]). The proximity tracing application exists entirely in the users' smartphones, keeps a detailed log of the contacts and communicates, when necessary, with a centralized or decentralized database that stores the anonymous identifiers of the infected people. As a result, it can inform the application users if they have been in contact with someone who has been identified as a confirmed infected case. Independently of the real (in-factum) efficiency of the proximity tracing methods, the pure contact tracing applications may belong to the first wave of healthcare applications for epidemic

[2] A. Crocker et al, 2020, The Challenge of Proximity Apps For COVID-19 Contact Tracing, Electronic Frontier Foundation avaialble at https://www.eff.org/deeplinks/2020/04/challenge-proximity-apps-covid-19-contact-tracing

[3] See for example, Euronews, 15.07.2020, Coronavirus: How is the EU preparing for a second wave?, at https://www.euronews.com/2020/07/15/coronavirus-how-is-the-eu-preparing-for-a-second-wave

[4] L. Di Domenico, 2020, Expected impact of lockdown in Île-de-France and possible exit strategies, INSERM (EPIcx lab), available at https://www.epicx-lab.com/uploads/9/6/9/4/9694133/inserm-covid-19_report_lockdown_idf-20200412.pdf

[5] The strategies under consideration mostly rely on experimentation and evidence-based policy methods to reduce the uncertainty that is inherent in the operation; in this regard, see in particular: K. Kupferschmidt, 2020, Ending coronavirus lockdowns will be a dangerous process of trial and error, Science, available at https://www.sciencemag.org/news/2020/04/ending-coronavirus-lockdowns-will-be-dangerous-process-trial-and-error#

[6] L. Ferreti et al, 2020, Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing, Science, available at https://science.sciencemag.org/content/early/2020/04/09/science.abb6936

[7] For a simple proximity-based approach to contact tracing, see: https://epic.org/privacy/covid/Rivest-Contact-Tracing.pdf; for an overview of the different privacy protocols used in tracing COVID-19 exposure, see: https://isc.sans.edu/forums/diary/Privacy+Preserving+Protocols+to+Trace+Covid19+Exposure/26066/; on the recent Google Apple contact tracing app, see: https://www.technologyreview.com/2020/05/04/1001060/google-and-apple-lay-out-rules-for-contact-tracing-apps/amp/

[8] A. Hassidim et al, 2016, Ephemeral Identifiers: Mitigating Tracking & Spoofing Threats to BLE Beacons, available at https://developers.google.com/beacons/eddystone-eid-preprint.pdf

tracking and observation. Next-wave applications with increasing product sophistication may yield improved contact tracing performance (through optimized proximity tracing and privacy-enhancing location tracking) and, include additional functionality such as integration with digital healthcare records, spatial risk analysis, and infection warning, digital methods[9] and recommendation actions for reducing infection risks, etc[10].

In this paper, we report on the design of a service system to endow next-generation COVID-19 mobile applications with the capacity: a) to instantly manage and verify a wide range of possible COVID-19 digital documents (circulation attestations, work or travel permits based on approved COVID-19 tests, vaccination certificates, etc.) and, b) to provide credential-based access control, especially in cases where the Verifier is not a web entity but a human agent with a smartphone, or an IoT device -- mainly in ad hoc outdoor and indoor settings. We envision the need of issuing and managing COVID-19 digital documents, with high-security safeguards, that will help policy-makers to design the conditions of work during a pandemic, and business managers to deploy contactless modes of organization[11] (such as, for example, remote staff onboarding and right to access specific location checks, work or travel permits for staff with digital credentials issued by a health authority, customer identity verification at the point of delivering customer service and so on). The system has been designed as a response to the specific needs of a health emergency situation, but it may have a broader application in different cased and areas of control (such as airport and train stations checking points and board controls), where the verification process must exclude the possibility of a physical interaction between the controller and the subject of control, by maintaining a "safe distance" between them and while preserving a certain privacy for the subject of control.

We embrace a fully privacy-protecting approach which builds on the recent developments in the area of Disposable Identities[12] and Verifiable Credentials[13] to enable COVID-19 digital document verification and credential-based access control in ad hoc outdoor and indoor settings (and beyond), on the basis of

[9] The online version of New York Times has recently made available an augmented reality experience tool available on mobile phones showing how show you how social distancing guidelines (i.e the rule of 2 meters of separation at minimum) can apply in real life, at a grocery store, on the sidewalk etc; see: https://www.nytimes.com/interactive/2020/04/14/science/coronavirus-transmission-cough-6-feet-ar-ul.html?referringSource=articleShare&fbclid=IwAR1mFko0uOZXRZT_T12AfsP56KcBHyKJ2q-f0UyKdxTKOPSWNjdh2La-xAk

[10] See as an example what is designed in Covid-watch project, especially the analysis of a mobile app to reduce the spread of COVID-19, composed of two parts, a "Bluetooth Contact Tracing" component and and a "User Recommendations: component (https://www.covid-watch.org/covid_watch_whitepaper.pdf)

[11] McKinsely predicts the rise of a contact-free economy and increasing automation where even the human-contact centric tasks needs to be automated as much as possible: "In effect, it is becoming possible to imagine a world of business—from the factory floor to the individual consumer—in which human contact is minimized. But not eliminated: for many people, getting back to normal will include popping into stores again, and the roadside kiosks typical of much of the developing world are not about to be replaced by cashless hyper stores. Patients with complex needs will still want to see their doctors in person, and many kinds of jobs are not automatable. But the trends are unmistakable—and probably irreversible...". See: McKinsey, 2020, The future is not what it used to be: Thoughts on the shape of the next normal, available at https://www.mckinsey.com/featured-insights/leadership/the-future-is-not-what-it-used-to-be-thoughts-on-the-shape-of-the-next-normal

[12] R. van Kranenburg. L. Anania and G. Le Gars, 2020, Disposable Identities, available at http://www.disposableidentities.eu (forthcoming)

[13] W3C, 2019, Verifiable Credentials Data Model 1.0, available at https://www.w3.org/TR/vc-data-model/

"derivative" (i.e., transcoded/contextual) Verifiable Credentials. A Derivative VC is a derived bond contract guaranteeing the validity and ownership over the underlying contracts (VCs) whose: a) usability is restricted in a very specific context (that of the "local" and time-limited interaction between a Subject and a Service Provider) and, b) linking table points only to a specific "Pairwise Decentralized Identifier" (DID)[14]. With sophisticated safeguards, like the issuance of different uncorrelated DIDs per person and decentralized cryptography, the service could offer strong privacy guarantees while promoting resilience and efficiency in use.

We present this design document to Data for Policy 2020 Conference, with the ambition to point to issues that should be addressed in order to innovatively adapt to a "new normal", and with the objective to contribute to the technology exploration which is expected to mark the upcoming months and years. Besides, we seek feedback from the public policy design and IT technology communities, especially from the experts and colleagues from the identity management and cryptography fields.

1 Digital COVID-19 certificates (permits, passes, etc.): the need to design "documents as applications" - key concepts

Not only is the digital monitoring of COVID-19 spreading a privacy concern, but it is also challenging established design principles for creating a mobile application. Usually, mobile phones are used to store e-documents, such as a boarding pass for an imminent flight, which are presented then, by the owner of the mobile phone, to a verification service (an airport gate controller for example), as proofs of an access right (in this example, boarding to the plane). In fact, very frequently, we allow a human agent seated in front of us to access, read or scan an e-document stored in our mobile phone (and displayed on the screen), as part of a request process to enter a public space (i.e., a museum), or to get access to a transportation mean (airplane, train, etc.). This may not be working in that way after the COVID-19 health crisis mainly due to social distancing requirements and restriction measures.

One of the problems faced recently, during the recent coronavirus lockdown, was the safe verification of the documents (circulation attestations and permits) that citizens were required to carry with them when leaving the house and going out for the essentials. In fact, several countries (Italy, France, Greece, etc.) had imposed special permission slips in the context of policies aiming at curbing the spread of the virus through the application of confinement and social isolation measures[15]. In another context, Chile, Britain and Estonia have mentioned the possibility of providing "immunity passports" to citizens with COVID-19 antibodies, to allow a certain return to the workplace[16]. This perspective is being discussed in the US

[14] W3C, 2020, Decentralized Identifiers (DIDs) v1.0, available at https://www.w3.org/TR/did-core/
[15] https://www.politico.eu/article/france-announces-stricter-coronavirus-confinement-rules/
[16] https://www.theregreview.org/2020/05/05/emamian-covid-19-immunity-papers/

policy-making community as well[17]. The issue of immunity passports became quickly controversial, with some experts pointing to the uncertainty over the level of antibodies that might be required for a person to be protected from a second COVID-19 case, as well as to medical privacy fears and the potential for abuse [18]. In contrast, the idea of a vaccination certificate is very welcomed by the scientific community[19]. As more and more countries around the world currently design strategies for applying different containment measures and managing local lockdowns, and carefully work on medium-term contingency plans, the issuance of COVID-19 related digital documents (especially when it is to provide customers with safety guarantees, as in the tourism industry, and protect the health of front-line workers and volunteers by enabling touchless entry access) may be increasingly present in the organization of whatever should be the "new normal"[20]. Generally speaking, the verification of all these documents when someone should access an "organized" private or a public "commons" area (as for example in the cases of an officer performing outdoor checks or controlling the entrance in transportation stations and ports, large shops, common infrastructures, etc.), and the conditions of their validity on the basis of a health or any other context specific attribute, may need special attention.

First, because of the ad hoc nature of the process of digital document verification: it frequently takes place in ad hoc locations, on a street, in an urban road in the context of a vehicle check, in a public location or even in a private building, not necessarily at the entry but somewhere else, if exceptional security measures should apply.

Second, because the verification in several cases is operated by humans, i.e. control officers, and this may imply a real risk of contamination for them, should they come in contact with an infected person or a contaminated object. France's Minister of the Interior Mr. Christophe Castaner, answering to why the verification process of the french *attestation pour sortir* did not initially happen electronically, using smartphones, but required from citizens to present a paper signed form, focused his response on the safety of the officers-verifiers (and the possible privacy flaws of the electronic process)[21]. Mobile phones are proven to harbor dangerous bacteria and viruses, making them a likely point of contamination for control officers and citizens. Given the high-risk of mobile phones microbiological contamination, should one return

[17] https://www.politico.com/news/2020/04/10/fauci-coronavirus-immunity-cards-for-americans-are-being-discussed-178784
[18] See for example:
https://www.statnews.com/2020/04/20/everything-we-know-about-coronavirus-immunity-and-antibodies-and-plenty-we-still-dont/ and
https://uk.reuters.com/article/health-coronavirus-technology/refile-experts-warn-high-tech-tools-to-fight-covid-19-pose-their-own-risks-idUKL8N2FX5Q1
[19] https://www.thelancet.com/journals/lancet/article/PIIS0140-6736(20)31034-5/fulltext
[20] A Working Group from the Covide Credential Initiative (https://www.covidcreds.com/) has defined several use cases of COVID-19 Digital Credentials, "in a format as close to the NHS digital passports as possible, but for civilians, non-NHS staff, giving priority to front-line workers and volunteers…"; see:
https://docs.google.com/document/d/14z7deFUHSI-x60KMLhF2FoxPIbCGmEMEJl0myr4g4dA/edit#.
For a detailed description of the format used in credentials issued by UK NHS, see:
https://drive.google.com/file/d/1_yiT059ACzThUhgKMU7Tq-8MsCeRd5QB/view?pli=1
[21] https://twitter.com/CCastaner/status/1240377676977897476

to paper documents and plastic cards? Of course, this is neither a good alternative (papers and plastic surfaces can support infectious viruses) nor a desirable outcome in the long-term[22]. Besides, the French Government has modified the position taken in the beginning, and it allowed later the generation of simple digital *attestations* by the citizens. The digital document generated online, contained a QR code which could be scanned by the police officers, in case of a control. The use of a QR code means the police officer does not actually need to touch the phone of the subject of the control; a portable image-based barcode scanner permits the capture of the mobile screen of the control subject with satisfactory reliability. However, the officer still needs to approach the subject close enough, at a distance that allows the scanner to adequately focus the QR code symbol clearly, thus eventually breaking the necessary "social distancing" rules.

Third, and more important, because the verification of a digital document, naturally, imposes additional privacy-preserving priorities and non-discrimination imperatives that should be strictly respected and implemented under an end-to-end privacy by design approach -- and may also require a minimalistic data disclosure, or even the guarantee of the anonymity of the subject of control.

How should one organize safely and efficiently a document verification process under such conditions?

1.1 Disposable Identity documents-as-applications

This paper discusses the **"social interface" and the different components of an application for automated e-document verification in outdoor and ad hoc indoor settings**. Basically, it designs the **appropriate modes of interaction** (service encounters) between the participants in a process of (digital) verification of a permit, certificate etc., which takes place in the public space (on the street, at the entrance of a transportation terminal, building, store etc.). Besides, we outline the necessary functionality of the **back-end infrastructure** which supports the "service encounters" taking place at the "front-stage".

Moreover, in this paper, we describe the **multi-layer architecture** of an **application with a broader functionality** (document-as-application) that can, a) manage the storage and the presentation (for verification) of COVID-19 related digital documents and permits (such as circulation attestations, work and travel permits, vaccination certificates etc.) and, b) provide support for integrating data into the digital documents it creates and processes. These data can be found outside of the application documents, for example in contact tracing applications, health databases, and other sources. The **design of this document-centric application** will follow the foundational principles of the **Self-Sovereign Identity (SSI)**

[22] Documents are artifacts that combine content, structure and presentation. Individuals, business and governments deal and transact by exchanging documents. Digital documents create a process efficiency and productivity gains from effective information management, in the same way that coordinated, or "orchestrated" flow of business processes and operations generates new forms of value for both the business and its customers (see: R. Glushko and T. McGrath, 2008, Document Engineering: Analyzing and Designing Documents for Business Informatics and Web Services, MIT Press).

technological trajectory[23]. We intent to apply the SSI framework for issuing and managing **"Disposable Identities"**[24].

Disposable identities (i.e., Disposable Proofs of Identity) are temporary **attribute-based identities integrated in a smart contract (in the large definition of the term) between a receiver and a supplier of a service**. They are conceived to work as safeguarded identities to protect from risks of privacy invasion.

- Disposable Identities, or Disposable Proofs of Identity, are:
  - **Context-specific**
    - Example: Use during a trip: go through check-in, boarding control, customs clearance, identification with a hotel, reservation through a platform like booking or Airbnb
  - **Time-limited**
    - Example: A Disposable Proof of Identity is valid from the day of its creation until the expiration date (then, it automatically moves to a Revocation List)
- Context-specific plus Time-limited mean:
  - Ephemeral Identities

Figure 1: Disposable Identities - Definition

Enabled by a Self-Sovereign Identity (SSI) architecture, disposable identities are capable of providing anonymized, near real time, tamper free and verifiable identity information. This is mainly achieved using **Disposable Yet Official Identities (DYOIs)**, a model of Disposable Identities **based on SSI architecture**

[23] Self-sovereign identity (SSI) is a fresh approach to decentralization of the management of personal data that gives users essential control of their data. SSI aims at establishing a much higher level of trust for the existing internet infrastructure, based on mechanisms that allow for the automated and verifiable identification of parties to a transaction, while at the same time reducing the costs involved in the current centralized trust building mechanisms. The guiding principle of SSI, i.e., ensure the control over their personal data, is mainly achieved by using Verifiable Credentials (VC). A VC is capable of representing all of the information that a physical credential represents, but additionally is tamper-evident and more trustworthy than a physical one since it can be cryptographically verified. A cryptographically authentic and non-repudiated VC can be used to automatically verify ownership over it, authenticity and non-repudiation, as well as the identity of the entity issuing it. In the subject of SSI and Verifiable Credentials., see in particular:
A. Mühle et al, 2018, A survey on essential components of a self-sovereign identity, available at https://arxiv.org/pdf/1807.06346.pdf
D. van Bokkem et al, 2019, Self-Sovereign Identity Solutions: The Necessity of Blockchain Technology, available at https://arxiv.org/pdf/1904.12816.pdf
F. Wang and P. De Filippi, 2020, Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion, available at https://www.frontiersin.org/articles/10.3389/fbloc.2019.00028/full

[24] R. van Kranenburg. L. Anania and G. Le Gars, 2020, Disposable Identities, available at http://www.disposableidentities.eu (forthcoming) and NGI Forward, 2020. D4.7 Innovation Summit Report, mimeo

and adopting the **principle of (unlinkable) DIDs** over which a person has ownership or control. Disposable Yet Official[25] Identities mean that:

- They can be issued by an official authority, but they are completely managed by the identity subject through a mobile wallet application, and stored in the citizens' mobile phones in an encrypted form.
- They can include accurate (official) personal health information, contain proximity tracing or location data, or anonymized GPS location data, but they are structurally "unlinkable" to the subject's personal (official) identity information (PII data or mobile ID).

1.2 Disposable Yet Official Identities (DYOIs)

In other terms, a Disposable yet Official Identity is made from service or domain specific personal data (location and proximity, health, employment, etc.), and allows the subject to prove ownership over these data, without permitting anybody else to make (present or future) correlations between them and the subject's true identity. Essentially, **a subject generates many purpose-oriented "disposable" credentials, which are linked to different DIDs** over which a person has ownership or control. The term Decentralized Identifier (DID) is used to describe an identifier[26] that is publically discoverable using for example a distributed ledger. However, the public nature of a DID should not be mistaken for a potential user tracing enabler. Indeed, user DIDs need not disclose anything more than endpoints and cryptographic public keys. Specifically, using **Pairwise DIDs or Peer DIDs**[27], subjects are able to generate new DIDs, on the fly, and securely and privately communicate with a party making correlations with other parties effectively impossible, thus implementing a privacy-by-design property. **Only the subject themselves can make the correlation between the different DID under their ownership (unlinkability)**[28].

To explain our argument, we assume that a Verifiable Credential (VC) is issued by an authoritative VC Issuer and consumed by Service Providers (aka VC Verifiers or Receivers) which accept "verifiable presentations" (containing proofs of credentials) made by VC holders. Verifiable presentations are packages of evidence created by holders to satisfy a Verifier's (SP) requirement[29]. They may deliver a

[25] Official in the sense defined by FATF (Financial Action Task Force), "distinct from broader concepts of personal and social identity that may be relevant for unofficial purposes (e.g., unregulated commercial or social, peer-to-peer interactions in person or on the Internet)". According to FATF, official identity is the specification of a unique natural person that is: a) based on characteristics (attributes or identifiers) of the person that establish a person's uniqueness in the population or particular context(s) and, b) recognised by the state for regulatory and other official purposes (FATF, 2020, Digital Identity, available at https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity.pdf)

[26] W3C, 2020, Decentralized Identifiers (DIDs) v1.0, available at https://www.w3.org/TR/did-core/

[27] W3C, 2020, Peer DID Method Specification, available at https://identity.foundation/peer-did-method-spec/

[28] As Denis "Jaromil" Roio intelligently explains, it doesn't really matter how decentralized a privacy-preserving design is, compared to another, but "how far are reaching the risks of data correlation…"; see: https://medium.com/@jaromil/why-proximity-tracing-is-important-and-its-integrity-should-be-contextual-2b46e5681a45

[29] According to W3C-issued Verifiable Credentials Data Model, a verifiable presentation is "a tamper-evident presentation encoded in such a way that authorship of the data can be trusted after a process of cryptographic verification;; certain types of verifiable presentations might contain data that is synthesized from, but do not contain, the original verifiable credentials (for example, zero-knowledge proofs). See: https://w3c.github.io/vc-data-model/#dfn-verifiable-presentations

single credential, a collection of credentials, or sets of specific data units (i.e. claims) derived from one or more credentials. If the Verifier is a web entity, the presentation of Verifiable Credentials is an automatic process supported by specific machine-to-machine communication protocols that enable direct online interconnection between the wallet of the VC holder, stored in VC holder's mobile device, and the IT premises of the Verifier.

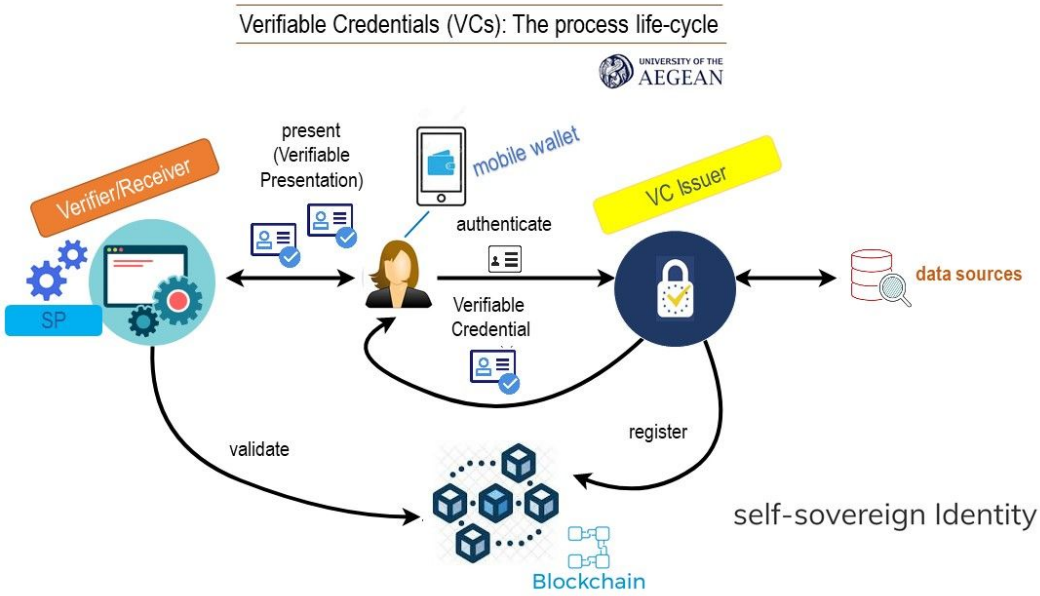

Figure 2: Verifiable Credentials - Issuance, Presentation, Validation

In more detail, we accept that a subject, Albertto, generates a DID (say DID1) to interact with some authority, VCissuer1, to create a Verifiable Credential, VC1, about themselves. Next, in order for Alberto to prove to a Service Provider (SPk) that he is in possession of some attribute, Att1, contained in VC1, Alberto generates for SPk a new DID, DID2, so that he can initiate secure (SSI standards-based) communication with SPk. DID 1 is in no way derivable from DID2. So there is no way for SPk and VCissuer1 to collude and trace Alberto's actions. Next, Alberto generates a Verifiable Presentation consisting of a Zero Knowledge Proof (ZKP)[30]. This proof allows Alberto to prove to SPk, irrefutably, that he is in possession of VC1, signed by VCissuer1, that contains Att1. This proof again leaks no information about the actual VC or the identifiers contained therein. It just allows for SPk to verify that Alberto is indeed in possession of this attribute[31]. This is presented in the following figure.

[30] https://w3c.github.io/vc-data-model/#zero-knowledge-proofs

[31] For a brief introduction of the use of Disposable Identities in the case of Health Certificates on COVID-19, see: R, van Kranenburg et al, 2020, Disposable ID - a new trust and privacy-based approach for Health Certificates on SARS-CoV-2, available at https://www.linkedin.com/pulse/disposable-id-new-trust-privacy-based-approach-health-mirko-ross. For a similar approach on the matter, which describes key technical and governance considerations necessary for a robust, privacy-protecting health credentialing system, see: D. Gruener, 2020, Immunity Certificates: If We Must Have Them, We Must Do It Right, Harvard Univ. Edmond J. Safra Center for Ethics | COVID-19 White Paper 8, available at https://ethics.harvard.edu/files/center-for-ethics/files/safracenterforethicswhitepaper8_1.pdf

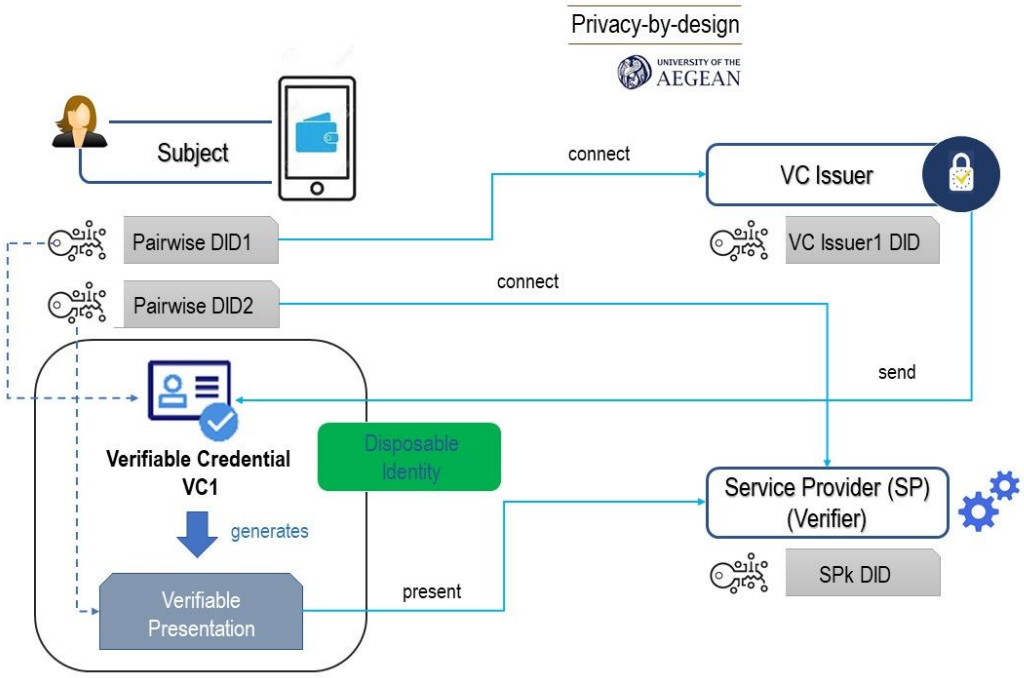

Figure 3: The use of "Pairwise DIDs" in the design of Disposable Identities

From the above example, it should be made clear **that the combination of Pairwise/Peer DIDs together with Verifiable Presentations based on ZKPs (Zero-Knowledge-Proofs) provides a sound foundation for a system that prohibits the tracing of the subjects' actions** and provides technological safeguards that exclude any possibility of linking DID data (unlinkability), and effectively dissuades a possible collusion between the different parties of the system, between the Issuers of Verifiable Credentials and the Verifiers (or SP providers), or among SPs, thus ex-ante implementing privacy-preserving design.

2. Digital document verification: operation models and types of services

In our perspective, digital and mobile-friendly COVID-19 work permits, travel passes and other related credentials are necessary artifacts for the application of "behavioral protocols" and other dynamic interventions that could support a smooth implementation of the selected disease containment strategies, including periodic (local or broader) lockdowns and lockdown-exit policies[32]. The term "behavioral protocols" is included in a recent report of McKinsey and refers to the specific organizational models and guidelines for operating businesses and providing government services under pandemic conditions[33]. With

[32] According to several recent studies, the different countries must be prepared for a few more months of significant COVID-19 activity, "with hot spots popping up periodically in diverse geographic areas"; see: (https://www.statnews.com/2020/05/01/three-potential-futures-for-covid-19/?campaign_id=154&emc=edit_cb_20200508&instance_id=18350&nl=coronavirus-briefing&regi_id=61766261&segment_id=27020&te=1&user_id=f4e35fa719e6e3ebc5c90b14f75bf9b0&fbclid=IwAR2RFv-URHSHmuCbmq3gMDgzezAjtPcN7duspKly_EHU8gB26eiTs73eQps).

[33] See in particular: McKinsey, 2020, Safeguarding our lives and our livelihoods: The imperative of our time, available at

reference to the ongoing situation, COVID-19 permits/certificates may for example help to effectively apply targeted restrictions in people movement (when and where it is necessary), to run critical infrastructures from workers with a lower risk of contamination (or immunity), and to provide business and government services activity through new forms of organization like work shift planning and other detailed physical-distancing and health protocols[34]. Like behavioral protocols, the digital documents managing these permits/certificates, should not be uniform but dynamic, tailored to specific needs and circumstances, adapted to the changing nature of the public health policies, eventually updated on changes of the health status of the document holder and, of course, securely and transparently verifiable to preserve people's privacy[35].

2.1 Operation models

Obviously, the challenge of designing digital documents in the context described above, rises from the **specific organization requirements of the document verification process** which should ensure security, privacy and physical safety.

As already explained, in most cases, a document verification process takes place in ad hoc outdoor and indoor settings, where a device with the capacity to scan barcodes directly from a mobile screen is not in general available. But, even if a portable scanner would be available to the controllers, the verification process must exclude the possibility of a physical interaction between the controller and the subject of control, by maintaining a "safe distance" between them. Therefore, an **electronic intermediary is needed to take the role of intermediary between the process constituents**. The design features specific to a fully "touchless" document verification process, as well as the management and deployment requirements, are listed through the two following, generic, Use Cases, a and b..

2.1.1 Use Case a: Digital Document Verification in ad hoc outdoor and indoor settings

https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/safeguarding-our-lives-and-our-livelihoods-the-imperative-of-our-time#

[34] McKinsey, 2020, Europe needs to prepare now to get back to work - safely, available at https://www.mckinsey.com/industries/public-sector/our-insights/europe-needs-to-prepare-now-to-get-back-to-work-safely?cid=other-eml-alt-mip-mck&hlkid=e990be4d26e84511ae2c05ace7405cf8&hctky=11915619&hdpid=7eb704c8-45b8-4bb8-be77-1594a67f7031

[35] The latter underlines the need to design COVID-19 digital credentials which can be used in ways that protect the personal data of the holder and the privacy of their use (against surveillance). Specifically, in the case of an ad hoc verification, the process should prevent on the one hand, the subjects of control from stigmatization (if a personal credential suddenly includes information that reveals an increased probability of health risk) and, on the other hand, as pointed out above, avoid exposing the verifiers to contamination risks. We reason here in accordance with the guidelines proposed by the European Commission in April 2020; see: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_626 & https://ec.europa.eu/info/sites/info/files/5_en_act_part1_v3.pdf

Use Case a Scenario: *During a temporary lockdown, Agnes needs to exit her residence to shop for groceries. Prior to leaving her residence, Agnes generates a permit for shopping by interacting with a central permit system. On the road to the shop, Agnes is stopped by a police officer and is asked to present her permit. She does so by transmitting her permit to the officer using her mobile phone without interacting physically with him (a minimum safety distance of 3m is respected). Next, the officer validates her identity and the permit and checks the timestamp of its creation. Agnes is allowed to proceed with her business without having revealed to the control officer any significant identity information.*

The successful design of an electronic intermediary capable to support a case scenario as described above, must establish two **core functionalities**.

First, ensure the **instant and contactless transfer of the proof of a digital document from one mobile phone to another**, from the cellphone of the subject of control to the control officer's mobile device.

Second, allow the mobile phone of the control officer to recognize the individual request of a subject of control and, by maintaining **separation of the processing of each individual request**, to select from a group of people (in real-time) those to whom access should be granted and those who do not possess the requested permit.

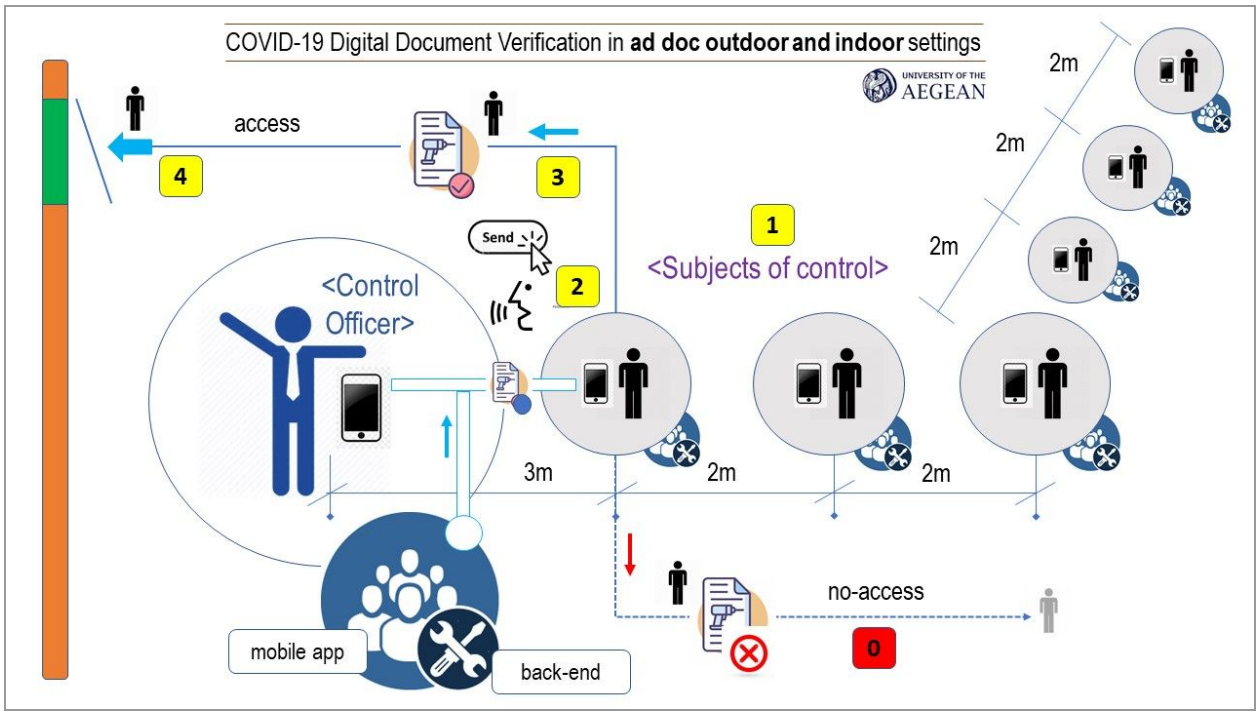

Figure 4: Use Case (a) - Process scheme

Digital Document Verification in ad hoc indoor and outdoor settings - Process Flow:

1. Check-in line (1)
    - Subjects of controls are arranged in a check-in single-server, single-phase line with a minimum distance between them.
2. Check-in preparation (2)
    - The control officer requests sequentially from all individuals waiting in the line to present a proof of possession of a valid, specific document (for example, an immunity pass) -- while constantly maintaining a safe distance from them.
    - The subject of control instantly creates, using their mobile app, a (tamper-evident) disposable credential-presentation[36] which contains a proof of owning a valid instance of the requested document; this process-specific credential-presentation derives from the disposable and other credentials already stored in the subject's mobile phone.
3. Check-in operation (3)
    - The subject of control transfers the credential-presentation to the device of the control officer (through a nearby available network), or might simply verbalizes it, in a way that allows the control officer to verify its validity (in all cases, the interaction between the two process participants does not require any physical contact or to come close each).
4. Check-out (4 or 0)
    - In the case of a successful verification by the control officer, the subject of control goes through the checkpoint and accesses the area behind it (4).
    - In the case of failed verification, the subject of control moves out of the check-in area without leaving any trace since the process guarantees the anonymity of the checked people checked-out (0).

2.1.2 Use Case b: Credential-based access authorization through a terminal or a portable device

In parallel, the **application-intermediary should work with any IoT device which can grant access to a specific area by performing automated document verification**. This may be the case of a **more structured document verification process** that takes place, for example, **at the entrance of a port or a passenger ship**, or, the case of a company which decides to temporarily remove the touch access systems and instead use a **remote method for secure entry**; and/or deploy **flexible ad hoc checkpoints** for better managing access control within a building, a factory, or a larger industrial area. A wide range of devices can operate a "spatially flexible" control, from simple tablets to fixed and portable mobile screen scanners. In this instance, the application of the subject of control should achieve interoperability with the data processing facilities and legacy IT systems of the control entity.

[36] In the form of a QR-code, a sheed phrase/word, or a bluetooth beacon (see below)

Use Case b Scenario: *Lucrezia needs to commute, using a ferry, to get to work. Before leaving home, she checks her phone app to ensure that her travel permit is still valid. On the port entrance she recognizes the queue for safe on-boarding. People stand in line, respecting social distance, and one by one use their phones on the installed terminal scanner at the end of the queue. A few meters behind a security officer ensures that all individuals truly scanned their phones and that their travel permits were successfully verified. When Lucrezia reaches a specific distance her phone app prompts her to generate a suitable presentation from her travel permit that she can use to interact with the terminal. This presentation discloses no information about Lucrezia to the system other than the fact that she is in possession of a valid permit. Upon reaching the terminal Lucrezia uses her phone to interact with the terminal. A green light flickers indicating she is allowed to pass through and Lucrezia enters the protected zone.*

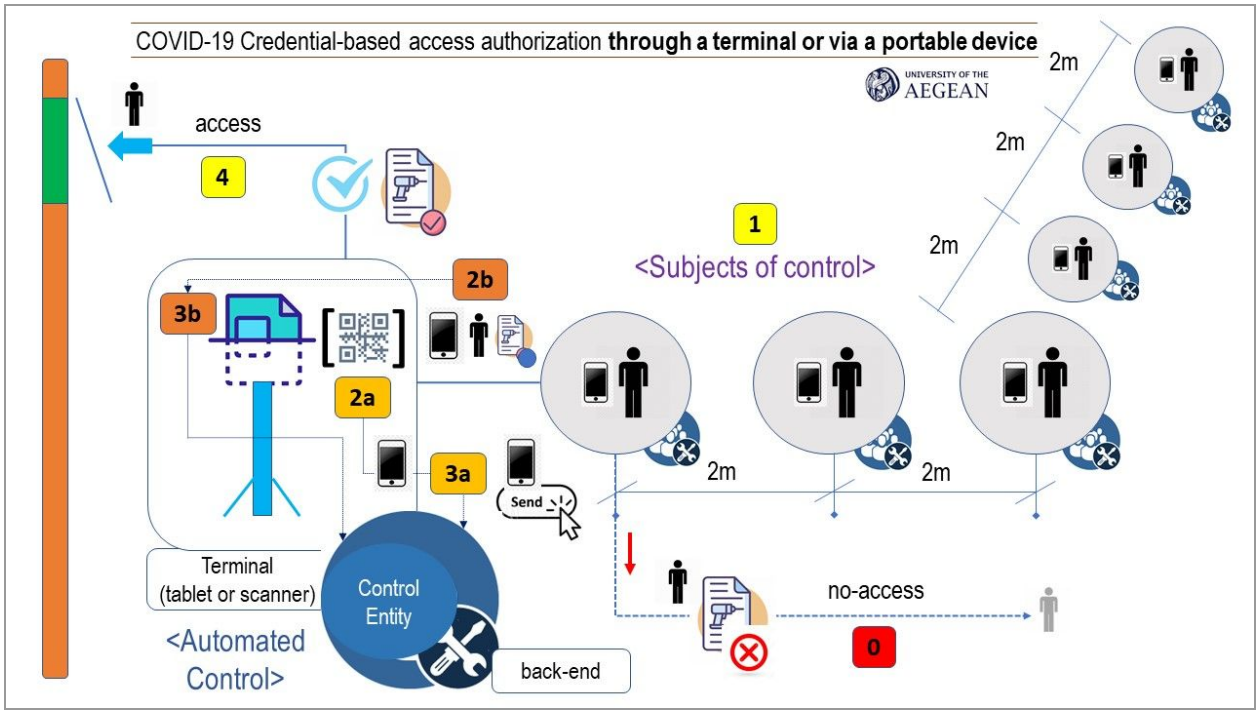

Figure 5: Use Case (b) - Process scheme

Credential-based access authorization through a terminal or via a portable device - Process Flow:

1. Check-in line (1)
    - Subjects of controls are arranged in a check-in single-server, single-phase line with a minimum distance between them. One by one, they approach the checkpoint and use their phones on the installed terminal, which can be either a simple device with a screen, such as a tablet, or a terminal scanner (cases a and b, respectively)
2. Check-in preparation (2)

- The subject of control scans one of the QR codes that automatically and consecutively flash and spin on the terminal (2a).
- The subject of control instantly creates, using their mobile phone, a (tamper-evident) disposable credential-presentation (in the form of a QR code or a bluetooth beacon)[37] which contains the proof of owning a valid instance of the requested document; this process-specific credential-presentation derives from the disposable and other credentials already stored in the subject's mobile phone (2b).

3. Check-in operation (3)
   - The application of the subject of control sends/presents the credential-presentation to the back-end system of the control entity (3a).
   - The subject of control approaches the terminal scanner and presents the QR code displayed on the screen of their mobile phone, or transfers the credential-presentation to the terminal through a nearby available network. The terminal captures/receives the credential-presentation sent by the subject of control and communicates with the back-end system of the control entity (3b).
4. Check-out (4 or 0)
   - The back-end system of the control entity verifies the authenticity, validity and ownership of the received credential-presentation and allows the subject of control to go through the checkpoint and accesses the area behind it (4).
   - In the case of failed verification, the subject of control moves out of the check-ın area without leaving any trace since the process guarantees the anonymity of the checked people checked-out (0).

2.2 Types of services

The service model of an application that allows for the instant verification of a digital document in outdoor and ad hoc indoor settings and, in a broader sense, allow for credentials-based access authorization, should support a variety of types of services (the previously designed operational models already provide an indication of the required diversity). Different **types of services are distinguished by different requirements for such things as data model, presentation and communication**. In fact, we need to define in detail:

1. Data models for the data to be transferred from the device of the subject of control to the mobile phone of a control officer or to an IoT device.
2. Presentation means, i.e., data presentation schemes.
3. Channels for data communication between the devices involved in the process.

[37] See section 2.2.2

2.2.1 Data models

As already mentioned, the physical credentials we frequently use in our daily life (from driver licenses to certificates and property titles, and from airplane and train tickets to passports and permits) are now available as digital files, in the form of e-documents, that can be stored in smartphones, indexed, retrieved and instantly presented to prove ownership of the original document. But e-documents are not necessarily valid as the original ones. To be considered as authentic, an e-document should either carry the digital signature of the document issuer, or be validated using a validation service. These methods guarantee that the content of the original document has not been altered, by using a cryptographic method to verify the authenticity and integrity of the e-document. While valuable and largely used, these methods were essentially designed for the pre-mobile Internet applications. The mobile Internet era requires that we can securely carry these digital credentials on smartphones, and provide validation methods on demand. In fact, today's digital credentials contain cryptographic powers that make them tamperproof, secure, and verifiable.

Schemas for digital credentials are now proliferating. It is however desirable to draw schemas from a standard inventory. **Verifiable Credentials (VC) as defined by the W3C Consortium**[38] in the context of an SSI ecosystem[39], are the most suitable solution for the problem studied here. They provide an out of the box and standardized way of verifying that the presented credential (i.e. a permit) is owned by an anonymous but "real" identity owner, issued by a trusted authority, and that the credential is still valid[40].

Else, a **custom JSON-LD (JWT encoded) structure** might keep the design of the credential cleaner and simpler and eventually used in the most extreme cases, where, for example, network availability issues do not allow the proper use of Verifiable Credentials (or in case where the comparative advantages of Verifiable Credentials[41] are not evaluated as important).

2.2.2 Available presentation means and transcoding

When digital credentials conform to the W3C's Verifiable Credentials Data Model, they are called Verifiable Credentials (VCs). As already pointed out, Verifiable Credentials (VC) are issued by an authoritative VC Issuer and consumed by Service Providers (aka VC Verifiers or Receivers) which accept "verifiable presentations" (containing proofs of credentials) made by VC holders. If the Verifier is a web entity, the presentation of Verifiable Credentials is an automatic process supported by specific machine-to-machine

[38] In short, a Verifiable Credential is a set of one or more claims made by an Issuer and stored in a mobile wallet owned by its holder. A verifiable credential is a tamper-evident credential that has authorship and can be cryptographically verified. For more information, see above (footnote #20) and: Verifiable Credentials Data Model 1.0 is a W3C Recommendation, at https://www.w3.org/blog/news/archives/8042

[39] See above

[40] Verifiable Credentials offer (in a nutshell): a) proof of the link among person and permit ownership, b) self-sovereignty, i.e. storage only on user's wallet and, c) in most implementations Zero-Knowledge-Proofs (ZPF), i.e., data minimization.

[41] See previous footnote

communication protocols[42] that enable direct online interconnection between the wallet of the VC holder (stored in the mobile device of the VC holder), and the IT premises of the Verifier. Generally speaking, digital credentials need to be generated in such a way that ensures that: a) they are bound to the individual (no swapping of documents), b) they guarantee that the identity of the entity issuing them is easily verifiable, c) they are tamper-proof, d) they can be separately revoked (if such a need arises) and, finally, f) they safeguard the privacy of the users. Currently, the most mature SSI technological frameworks (Hyperledger Aries, Sovrin etc.) guarantee these features and provide credibility to a Verifiable Credentials-based approach[43].

However, **in the operation models where the Verifier is either a natural person holding a mobile phone (e.g, a control officer) or an IoT device, complementary presentation means are needed to ensure that the content of a Verifiable Credential can be properly understood by the Receiver/Verifier.** For this reason, an **additional protocol layer** should be deployed to allow a credential-based verification process to handle this additional constraint. Basically, the process should become capable of instantly transforming an original Verifiable Credential to a secure cyber-physical VC, in other words to a **Derivative (or contextual) Credential,** disposable by default.

Specifically, the system we design in this paper works by introducing a **VC Transformation Service** to a typical SSI-VC verification process architecture. This component is contacted by the subject's wallet in order to generate **a very limited (in the sense of time to live and space to live) security token**. These tokens are easily interpretable by both humans and machines. An example of such a token could be a QR code, a 6 digit number or a word selected from a predefined list. What is very important to clarify here is that the validity of these tokens is affected by their context, i.e. the when and where they are used. Because they are **context sensitive,** generating such an operation-specific token from Verifiable Credentials is much more secure and feasible.

In more detail, once a subject is required to proceed with a credential presentation, their mobile wallet, after receiving a "VC Disclosure Request" by a Verifier, asks the subject to consent to the disclosure of a suitable credential. This request is resolved by the Verifier that validates the ownership, authenticity and validity of the submitted credential without revealing any traceable information about the user to the system. If a process requires **specific types of Credentials**, such as the short-living tokens described above, **their issuance can be handled in a similar way**. A specific online service, a **VC Transformation Service** can be created which transcodes existing Verifiable Credentials (VCs) into a suitable security token (derivative Credentials) and propagates it back to the subject's wallet. In this way, a **Verifiable Credential is used as**

[42] Such as the Aries Present Proof Protocol 1.0 (RFC 0037); see in particular: https://github.com/hyperledger/aries-rfcs/blob/master/features/0037-present-proof/README.md

[43] Zenroom can also provide support to a credential-based access control operation. Zenroom is a free and open source VM software, supporting Attribute Based Credentials (ABC) and non-interactive zero knowledge proof (zk-SNARKS) based on Coconut, a selective disclosure credential scheme (https://arxiv.org/pdf/1802.07344.pdf).

the key for generating a short-lived cyber physical access token. Having received this token, the mobile wallet of the subject can use it to **presentate it in various operations and usage scenarios**. Validation of these access tokens is straightforward as the receiving party needs only cross reference the received token with a list of valid codes received from the VC Transformation Service. Very likely, **QR codes**, **seed phrases/words** and **BLE beacons (advertising packets)** are the potential presentation formats into which Verifiable Credentials should be transcoded, to address the specific needs of an ad hoc digital document verification and credential-based access control operation[44].

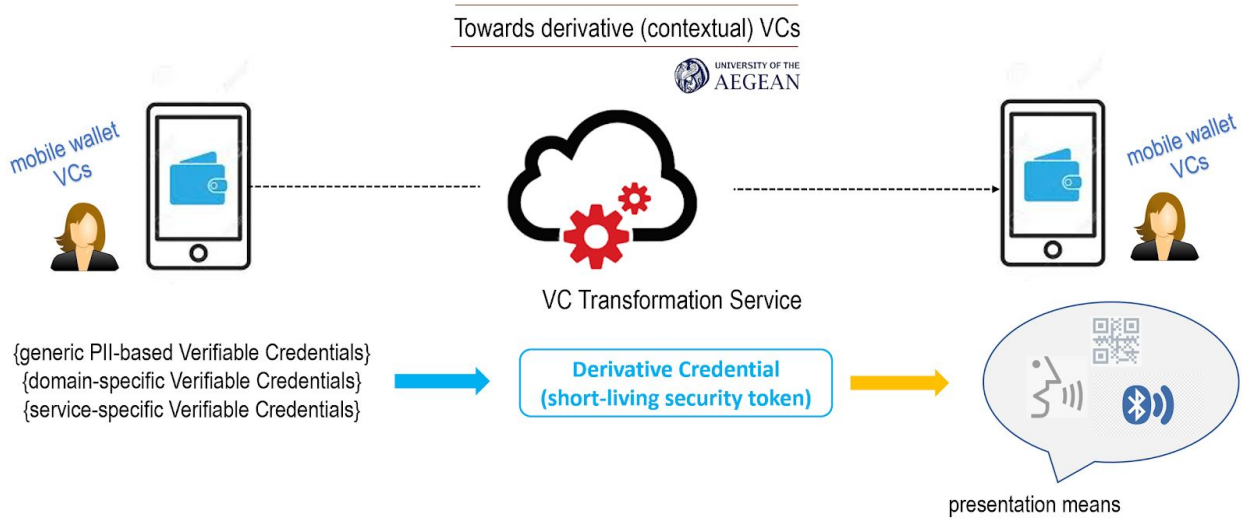

Figure 6: The organization of the issuance of Derivative VCs

2.2.2.1 QR codes and QR code scanning

QR code is the trademark for a two-dimensional barcode[45]. This is the most frequently used solution for initiating a "VC presentation session"[46] in an SSI environment. Very often, a user is invited to scan with her mobile phone a (projected to a screen or surface) QR code containing a Verifiable Credential (VC) request from a SP/Verifier. Immediately, the user's mobile wallet receives the VC request and selects which VC(s) to present to satisfy the request of the SP. The SP receives the "presented VC(s)" and validates VC(s)'s authenticity, ownership and expiration time.

In another setting, a QR code can be used to transcode the Verifiable Credentials made on the basis of W3C standards into simple formats that can be transferred from one device to another without necessarily relying on the mobile network. QR codes in such a context seem to work well in the case, for example, of a mobile screen displaying a QR code and a scanner reading the QR code information. This is what exactly

[44] A similar transcoding process may apply in the case of a digital document represented by a simple custom JSON-LD (JWT encoded) structure (see Section 2,2.1)

[45] https://www.academia.edu/download/51791265/Three_QR_Code.pdf

[46] As already discussed, a (verifiable) presentation is the submission of a Verifiable Credential to a Verifier in "a way that authorship of the data can be trusted after a process of cryptographic verification"; see W3C, 2019, Verifiable Credentials Implementation Guidelines 1.0, op.cit.

happens with QR code-based boarding passes presented by the passengers at the airports' security checkpoints and gate facilities. However, the effective scan of a QR code, depends on the scanning distance, which cannot be greater than 50cm, and it slightly varies as a function of the device performing the scanning and the size of the QR code[47]. This is not an issue in the case of an automated access authorization where the requester of access can approach close enough the IoT device performing the scanning. It works less effectively when the control officer should use a portable scanner to validate a digital credential (i.e. a previously trancoded VC into a QR code), since the officer is forced to break the rules of social distancing, which may have dire consequences.

2.2.2.2 Seed phrases (and words)

Seed (or mnemonic) phrase is a randomized list of words of different length which may be cryptographically linked to the possession of a Verifiable Credential (VC)[48]. Seed phrases are commonly used to provide access or recovery of a Bitcoin or Ethereum wallet (they are selected from a 2048-word dictionary where each word determines a specific number)[49].

A seed phrase, compiled from private or extended private BIP44 HD[50] key for more convenient storage, can be used, in this case, as a transcoding format for a Verifiable Credential. In other words, the transcoding process will produce a minimal VC representation (a seed phrase or even, a single word representing a seed phrase) which can reveal to a control officer the essential features ("pass or not" and expiration date) of the credential carried by the subject of control. The subject of control digitally forwards the word or the entire sequence of words, to the control officer through a nearby network (mobile or bluetooth), or simply verbalizes it. The control officer can recognize the possession of an access right (that is included in the initial VC), since he/she receives the same word (or sequence of words) in his/her mobile phone. If the word (or phrase) presented by the subject of control matches that received by the control officer, the officer will grant to the subject of control the authorization for access.

2.2.2.3 BLE beacons (BLE advertising packets)

Bluetooth Low Energy[51] advertising packets are periodically broadcasted (in small time intervals) by mobile devices equipped with BLE transceivers and the appropriate software stack. They are used for advertising and discovering devices without prior connection state. In this sense, they can support a connectionless mode of communication between devices, if they are engineered properly. BLE advertising packets contain

[47] It depends essentially on the CMOS camera sensors capability and the data scheme of the QR code.
[48] https://themerkle.com/what-is-a-mnemonic-seed/
[49] https://hackernoon.com/how-to-keep-your-seed-phrase-safe-tk1kk3tgx
[50] https://github.com/bitcoin/bips/blob/master/bip-0044.mediawiki
[51] Bluetooth Low Energy (BLE) is a wireless technology used in several applications, from IoT, to smart cities, smart homes, e-health etc; more more details, see, C. Gomez et al, 2012, Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-Power Wireless Technology, available at https://www.mdpi.com/1424-8220/12/9/11734/pdf). The way BLE operates is through a specific broadcasting model: when a BLE peripheral device is turned on, it periodically sends "broadcast packets" on specific advertising channels to indicate to other devices that it is up and ready to receive connections. At the same time, a BLE device is supposed to scan the anbient frequency space ("listen") to explore upcoming connectivity opportunities.

information such as Preamble and Access Address, plus a protocol data unit that consists of a Header, an Advertiser Address, a Data Packet Unit (payload) and, a CRC field (the error detecting code for a bluetooth communication). The advertising packet data payload is the most interesting part of the BLE specification from an application point of view. It includes three essential fields:

- A Bluetooth Identifier, identifying the packet itself. It is a 16-bytes UUID (Universally Unique Identifier) which is allocated to each BLE hardware beacon manufacturer through a process similar to the MAC address assignment in network devices[52], or it is adopted by a specific software application that deploys a beacon functionality.
- A Signal (TX) power which indicates the expected signal one meter from the device. It is used to make distance estimates.
- Two important values, a Major and a Minor number (4-bytes in total) that are numbers assigned to each packet to help the receiver to identify separate BLE packet broadcasts within the same UUID domain, thus completing the functionality of the Bluetooth Identifier; in a custom design, these fields can be used for effective data transmission[53].

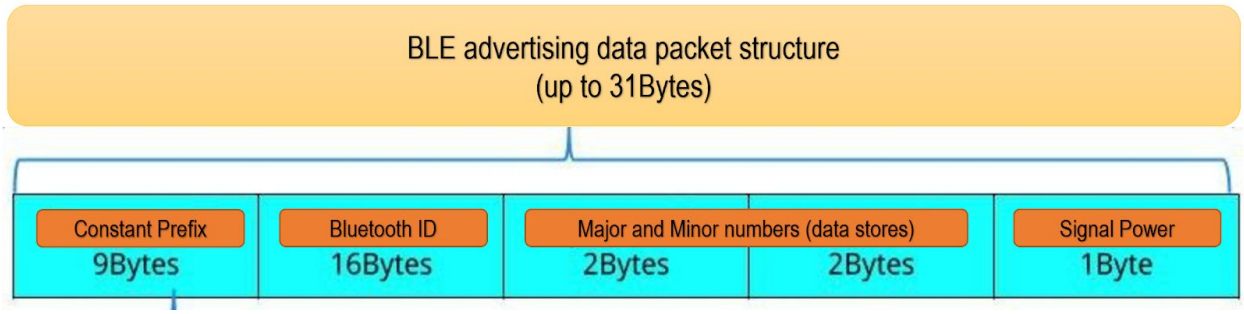

Figure 7: The structure of a BLE advertising packet

Currently, the mobile operating systems designers provide that help to BLE application developers through proprietary SDKs used to programmatically access the BLE broadcast transmitting and receiving functionality. BLE SDKs offer a development environment with specifications that, among others, economize over unnecessary battery consumption. These specifications are updated frequently to support an adequate security and privacy policy. For example, the initial privacy specifications for BLE advertising packets required the randomization of the Bluetooth MAC address in the BLE advertising packet header of each broadcasted BLE packet, but accepted that the same packet could carry a unique static UUID Identifier value in the packet data payload section. Over time, the initial specification has been modified to incorporate the concept of Ephemeral Identifiers (EIDs), which replaces the previously static 16 byte UUID identifier concept by a new type of identifiers, dynamically updated ephemeral UUID identifiers per broadcast packet which provide a significant privacy enhancement. The Ephemeral Identifiers are

[52] https://www.bluetooth.com/specifications/assigned-numbers/company-identifiers/
[53] See below

temporary identifiers, periodically changing and generated through cryptographic means and can only be linked back to the BLE packet[54]. Typically, a set of Ephemeral IDs correspond to a daily cryptographic key derived from a starting identity key, through chain hashing; a symmetric cipher in counter mode encryption operation and pseudo random generators are used to provide the daily set of unique Ephemeral IDs that populate the UUID 16-byte field of a BLE advertising packet. As a result, the application creates an ephemeral identifier for each packet, or for a small group of BLE advertising packets, that changes every few minutes. Of course, the broadcasted Ephemeral ID can be resolved remotely by the owner of the daily cryptographic key which generated it. Nevertheless, as far as the receiving device is concerned, an Ephemeral ID looks like a uniquely random ID.

Major mobile operating systems vendors like Apple (iOS) and Google (Android) support the use of Ephemeral Identifiers (EIDs) in their latest versions of the mobile platform development SDKs. However, each vendor follows a different approach. Apple allows for the generation of Ephemeral IDs automatically through the SDK native operating system functions[55]. Google provides an extensive support for rolling Ephemeral IDs through the Eddystone beacon (i.e., BLE broadcast packets) format specification[56]. Furthermore, both mobile operating systems impose restrictions at two important levels: a) the intervals between BLE advertising packet broadcasts and, b) the transmission capacity when the application is executing in the background[57]. Nevertheless, the recently formed Apple Google Consortium[58] has announced the development of a new design for Bluetooth Identifiers and common specifications for BLE broadcast packets to improve the privacy framework for the emerging contact tracing applications[59]. It is expected that the upcoming (updated) versions of iOS and Android mobile operating systems will provide the application developers with new Bluetooth APIs permitting the systematic creation and management of Ephemeral IDs, the cross-platform (interoperable) reception and transmission of BLE broadcast packets from mobile apps executing in the background, and a new broadcast beacon binary structure format that would be fully interoperable and recognizable by both platforms.

In sum, the generalized use of Ephemeral IDs, enabled by technological innovation and increasing interoperability between the two principal mobile worlds, and the careful design of a data transfer protocol for connectionless communication between mobile devices, based on the transmission of BLE advertising

---

[54] A. Hassidim et al, 2016, Ephemeral Identifiers: Mitigating Tracking & Spoofing Threats to BLE Beacons, available at https://developers.google.com/beacons/eddystone-eid-preprint.pdf

[55] https://developer.apple.com/documentation/corelocation/turning_an_ios_device_into_an_ibeacon_device

[56] https://developers.google.com/beacons/eddystone

[57] Specifically where the Apple iOS platform is concerned, a mobile app can receive and process in the background BLE broadcast beacons advertising but only from a limited number of distinct application registered UUIDs. And, the same iOS app, iis capable of transmitting beacons (with an unlimited number of varying UUIDs) only when it is executing in the foreground, as the result of a conscious choice of the holder of the mobile phone.

[58] https://www.ft.com/content/8a11bf86-dd71-4fd2-b196-e3ddffe48936

[59] https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ContactTracing-BluetoothSpecificationv1.1.pdf

packets (further described in Section 3.4), can transform BLE beacons to an effective carrier of transcoded Verifiable Credentials.

2.2.3 Communication channels

QR codes, seed phrases and BLE packets (beacons) can be exchanged automatically between two mobile devices and, consequently, between the participants in an ad hoc document verification process:

I. Instantly by using the **Bluetooth (BLE) protocol**, as a **Personal Area Network (PAN)** for a direct transfer of data.
II. Indirectly, through the **back-end communication infrastructure** that connects two mobile devices, which essentially is the mobile network together with the IT systems supporting the applications involved in the process.

The **first option (BLE network)** provides the framework to design and develop an effective connectionless service for transferring transcoded Verifiable Credentials (VCs) from their holder to a nearby control officer, **within a de facto secure micro-perimeter**. The **second option**, allows to systematically operate an automated document verification process inside a **custom defined control area** by a qualified officer using the techniques of **Geofencing**.

The Bluetooth channel is naturally used for establishing wireless Personal Area Networks (PANs) communications[60]. It is implied from what is already presented that the protocol has been specifically designed to support a wide range of short distances between two mobile devices. The effective distance depends on several factors, such as the available radio spectrum for digital modulation scheme, the transceiver antenna technology, the output power of the device etc. Bluetooth is a relatively secure protocol and, in general, it may operate at significant data rates, but consumes battery life quickly. Current mobile devices and wearables use a specific version of Bluetooth protocol, the Bluetooth Low Energy (BLE) specification. BLE uses a simpler digital modulation scheme resulting in smaller attainable data exchange rates to achieve a very low battery consumption. BLE provides actual payload data exchange rates approximating to 500Kbps in noisy environments, at a maximum approximate coverage of 30 meters, depending on the antenna quality characteristics of the device.

[60] Near-field communication (NFC), a set of communication protocols for communication between two mobile devices, could also be an option but it applies only over a very short distance (of 20 centimeters, when high power transceivers are used, or less, which is a more common situation). An NFC communication can be properly achieved between a smartphone (or a wearable) and NFC tags, or between a smartphone/wearable and stationed or mobile active NFC transceiver stations (such stations are commonly deployed at cash desks on large retail stores), or between a smartphone/wearable and an electronic payment terminal (POS). In addition, only a very small percentage of mobile phones allows mobile apps to programmatically access the NFC functions and exchange data with other NFC-enabled devices. As a result, NFC communication cannot be really useful in the present case where the mobile devices of the control officer and the subject of control should exchange data directly.

Geofencing is a location-based service in which an app uses the cellular network to trigger a pre-programmed action when a mobile device enters a virtual boundary set up around a geographical location, known as a geofence[61]. A geofence is a virtual perimeter of a real-world geographic area. It can be a radius (up to a few kilometers) around a location or a dynamically generated set of boundaries, traced as a (geo) polygon area in an enterprise GIS enabled infrastructure backend. A geofencing is a virtual barrier application that allows an administrator to set up triggers when the device of a host enters the area defined by the administrator so that a pre-structured communication protocol can be established between the devices of the administrator and the host. In practice, Geofencing is a technology used to monitor different mobile objects (persons, vehicles, tags), located by a cellular network. In fact, Geofences have a wide range of uses and applications from urban transportation to marketing. Public transportation systems deploy geofences to support multiple scenarios of user interaction in bus stations and to show bus locations in real time. Uber app assigns rides to the drivers closest to the user's perimeter or location. Walmart, to give another example, sends e-coupons to the customers based on their relative location (i.e., department) in their stores[62]. Obviously, there are several opportunities and benefits arising from using geofencing technology but there are also privacy concerns. As the users need to disclose some of their personal information, significant privacy risks can arise that may need mitigation actions. Compared to other emerging technologies such as BLE beacons, which provide location data only in micro-perimeters, Geofencing can apply at a larger scale and in many different areas within a city (pedestrian zones, squares and commercial centers, entry spaces in large buildings, city and peripheral streets with cars, etc.)[63].

3. Disposable Yet Official Identities (DYOIs) for ad hoc document verification and credential-based access control: a framework for balancing operational efficiency and privacy-preserving effectiveness

We assume:

- An application provider that provides SSI wallets to subjects (i e., the users of the application).
- An authorized government agency which is responsible for the issuance of COVID-19 health certificates ("negatively tested" status, vaccination certificate etc.)[64].
- Different business issuers of work/access permits based on the "behavioral protocols" applied by a company.

[61] A. Kupper et al, 2011, Geofencing and Background Tracking - The Next Features in LBSs, available at https://www.user.tu-berlin.de/komm/CD/paper/010221.pdf

[62] https://preyproject.com/blog/en/geofencing-7-commercial-and-industrial-use-cases/

[63] https://medium.com/@indianappd/advantages-and-disadvantages-of-geofencing-applications-a20e47bd2cc4

[64] In a generalized case, it can be any Issuer of context specific attributes, for example the Issuer of property titles or the Organizer of a big athletic event

- A proximity tracking mobile application which interacts with the wallet of the subject to eventually influence the "status" of the subject (a recently tested subject as "negative" is granted a work-permit but this may be "weakened", i.e.. changing from green to orange, if the subject came in contact with infected individuals).
- Service Providers that accept and verify the credentials presented by the subjects, and accordingly provide the requested authorization for access (examples: a Police Service, an airport or a train station, the organizers of an outdoor event, a specific company or a third-party provider collaborating with the company, etc.).

3.1 Multiple DIDs per person as privacy safeguards

A Disposable Yet Official Identity (DYOI) realizing the ad hoc document verification and credential-based access control requires a **small number of Verifiable Credentials anchored on four (at least) different types of DIDs (Decentralized Identifiers)**[65]:

1. A Health DID which is used by Verifiable Credentials pointing to the subject's health status.
2. A (set of) COVID-pass DID of the subject pointing out to data related to the access the subject may have in different workplaces and public transportation means.
3. A Personal Identity DID which is used by Verifiable Credentials pointing to the subject's PII data (always encrypted with a private key managed by the subject); this should be, in principle, different from any previously issued DID for the purposes of other SSI applications (i.e. civil identity, passport, student identity etc.).
4. A set of DIDs for interacting with Service Providers. These DIDs are different from each other and used by the subject when interacting with a Service Provider (they should be different from the DIDs described above, to ensure no tracing of the subject is possible).

The Health DID can be stored in a public blockchain -- potentially in a permission blockchain provided by national (or european) Health authorities, or in a government-sponsored blockchain. The COVID-pass DID is also presumably stored in a public blockchain. The Personal Identity DID can be stored in a public blockchain or in a government-sponsored blockchain. A pair of any of these three DIDs is never presented to any party, thus preventing possible correlations and ensuring the protection of the privacy of the subjects.

A subject might be issued and store in their mobile wallet the following types of Verifiable Credentials, provided by different VC Issuers (and stored in the subject's wallet):

[65] We reason here with reference to the "purpose limitation" design concept; see: http://www.isitethical.eu/portfolio-item/purpose-limitation/).

- A Verifiable Credential based on the subject's PII data (Identity VC): this is a type of VC containing the subject's personal identity information (the main data set of their national digital identity, or the eIDAS eID minimum data set) - anchored in the subject's Personal Identity DID.
- A Verifiable Credential issued by a Health Provider (Health VC) containing the subject's health status attribute (immunity, tested negative at this date etc.) - anchored in the subject's Health DID.
- Work Permit/Access type Verifiable Credentials, i.e., COVID documents granting access privileges (Work Permit/Access VC) issued by a company or a business VC Issuer mandated by a company to issue work- on its behalf - anchored in subject's COVID-pass DID.
    - The status of these credentials may automatically adapt to the information received by the proximity app which also runs in the subject's mobile phone and connects to the subject's wallet; a work-permit may be automatically withdrawn, or canceled for a number of days, if the contact tracing app reveals proximity of the subject with infected people that poses a threat to public health.
- A GDPR Consent Verifiable Credential (Consent VC): this VC is generated by the user's wallet app (signed using a Service Provider associated key) -- anchored in a public blockchain.
    - This VC expresses the consent given by the subject to a specific Service Provider to process the subject's data and associate them with their health status for as long as the crisis lasts (the user will be able to revoke this consent). This consent VC has as its subject the Service Provider's DID and is issued by the subject (self-issued).
    - A subject can create as many Consent VCs as the Service Providers the subject interacts with.

Issuers of Verifiable Credentials may be the owners of the original data which populate a subject's Verifiable Credential, such as the authoritative data sources providing the subject' health status (i.e., an authorized Health Provider) or the subject's identity (i.e., a national IdP or Service Providers over the eIDAS eID Network). However, we expect the emergence of a new species in the industrial space, a VC Issuer which will have the authority to issue Verifiable Credentials eventually regulated in a similar way QTSPs are currently regulated (against a Common Criteria Protection Profile)[66].

In order to ensure **privacy by design**, the **interactions of the subject with the various entities should be uncorrelated**. And at the very least, the system design should not allow for any entity to link the subject's PII with any other data, unless the subject explicitly authorizes it (e.g. by presenting both Identity and Work Permit/Access VCs to some entity). And even in that case, no other entity should be able to make any further correlations. To achieve these goals, we have already argued that **Pairwise or P2P DIDs should be used**[67]. This effectively means that the Subjects using their wallets should be capable of

[66] In this regard, see in particular: P. Kavassalis, P. Georgakopoulos and N. Triantafyllou, 2019, presentation at "Crypto Theory and Practices: Knowledge Building, Workshop, ENISA, Athens, November; available at https://docs.google.com/presentation/d/1u19UpMghMXhBF8DZEFuusDaw1VBY7uGbdRWo6qW0SdE/edit?usp=sharing

[67] See above: section 1.2

automatically generating new DIDs for the interaction with each different entity of the system, be they Issuers or Service Providers. Thus even if the entities of the system collude, they will not be able to trace the interactions of the users between them. However, the subject can at any time prove their ownership over all of these DIDs if requested (e.g. when presenting a VC issued to them).

- A subject can generate many purpose-oriented "disposable" Verifiable Credentials (Disposable Proofs of Identity) which are linked to different DIDs over which a person has ownership or control
  - Using **Pairwise DIDs** or Peer DIDs, subjects are able to generate new DIDs, on the fly, and securely and privately communicate with a party making correlations with other parties effectively impossible, thus implementing a **privacy-by-design** property
  - **Only the subject** themselves can make the correlation between the different DID under their ownership (unlinkability)
  - The **combination of Pairwise/Peer DIDs together with Verifiable Presentations based on ZKPs** (Zero-Knowledge-Proofs) provides a sound foundation for a system that prohibits the tracing of the subjects actions' and provides technological safeguards that exclude any possibility of linking DID data (unlinkability), and effectively dissuades a possible collusion between the different parties of the system

Figure 8: Disposable Identities and Pairwise DIDs - Summary

Specifically, there may exist **four types of Pairwise DIDs** for the subjects of the system corresponding to the four DID types described in the start of this section:

- Pairwise Health DID, generated upon pairing with a Health Provider
- Pairwise COVID-pass DID, generated upon pairing with a company or a business granting access privileges (associated with a Work Permit/Access)
- Pairwise Personal Identity DID, generated upon pairing with an Authority to issue an Identity VC
- Pairwise Service Provider interaction DIDs, generated upon pairing with the various Service Providers (SPs)

These DIDs are used in order to both issue and present the Verifiable Credentials described above. **For example**, **in order for the subject to enter a protected hospital area**, they are required to present **a Work Permit VC and a specific Health VC** (such as a recent time stamped immunity credential). The access-granting process takes place as follows:

1. The Subjects Wallet generates a fresh DID to interact with the Service Provider controlling access to company's premises
2. The Subjects Wallet generates a Verifiable Presentation based on the Work Permit VC and Health VC, essentially a "minimal" proof for the Service Provider that the Subject is in possession of a valid Work Permit VC and of a valid immunity pass, verifiable in such a way that does not disclose

the DIDs used for the issuance of these VCs, and disclosing no additional information about the Subject.

3. The Service Provider, verifies the received Verifiable Presentation and grants access to the Subject accordingly.

3.2 The "verifiable presentation" process makes an identity credential disposable

Disposable Identities are defined in the previous sections as attribute based identities integrated upon a digital contract between the receiver and supplier of a service. Furthermore, we have introduced the concept of Disposable Yet Official Identities (DYOIs), meaning that these digital contracts are anchored to an authoritative source. Indeed, all the interaction of the Subject with the Service Providers in the credential system takes place over Verifiable Presentations (VP) using Pairwise DIDs (i.e., an Identifier generated only for this specific context). Accordingly, a **Verifiable Presentation (VP), generated via Zero-Knowledge Proofs (ZPF),** or a Derivative VP (i.e. presentation of transcoded/contextual credentials) [68], **is a derived bond contract guaranteeing the validity and ownership over the underlying contracts (VCs)** whose: a) **usability is restricted in a very specific context** (that of the ongoing interaction between Subject and Service Provider) and, b) **linking table points only** to a specific Pairwise DID. Outside of this context, a Verifiable Presentation (VP) is useless, rendering it effectively disposable. Putting it in another way, **it is the specific presentation process that makes the "underlying VCs" disposable, and their undeniable association with official identity documents that makes them "yet official"**.

- A Verifiable Presentation links the attributes of a Disposable Identity to the attributes of an Official Identity
  a. **Validates** an identity presentation while ensuring anonymity
     - Example: The person presenting a disposable identity proof is a real natural (or legal) person under EU/national law
  b. **Integrates** attributes from different identities (i.e., attributes from a Disposable Identity and from an Official Identity) to a joint "Verifiable Presentation"
     - Example: The airplane ticket (a right to board the flight A3121) is linked to person X' "official" identity attributes [name, surname, uniqueID]
- But the "linking" is not provided by a Service; only the Subject, **if requested**, can create and present links between different Disposable Identities, or between a Disposable Identity and an Official Identity
- **Disposable Identities** are structurally **"unlinkable"** to the Subject's personal (official) identity information (PII data or mobile ID)

Figure 9: What a Verifiable Presentation really does?

In short, a Disposable Yet Official Identity (DYOI) has the following main characteristics:

[68] See above: section 2.2.2

- It is an **temporary and context-specific identity**, in the sense that it is meant to be discarded after the passing of the reason for which it was created.
- It is **anonymous**, in the sense that critical personal data (such as the subject's health status and how its is influenced by the activity of the proximity tracing app) are anonymized by design as they are contained in different VCs from the one containing the subject's personal data (the monitoring of the subjects' health status and the granting of specific privileges such as circulation, access etc. are necessary for the effective dealing with a pandemic, but this does not mean that the subject's personal data have to be exposed).
- It is an **official** identity, in the sense that it uniquely characterizes its possessor and is issued by an authoritative source.
- It is **dynamic**, in the sense that the subject's status and access privileges are time stamped and, as a result, it reflects the evolution (in real-time) of a subject's condition during a particular period of time.

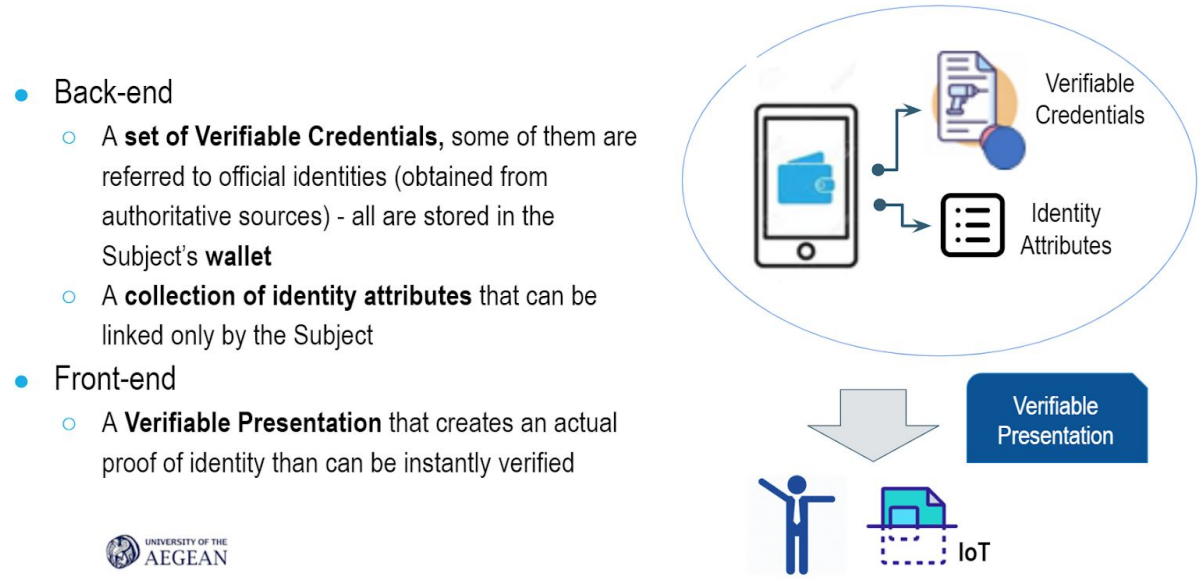

Figure 10: A Disposable (Proof of) Identity in a nutshell

3.3 Credential-based access authorization with use of a portable device (DYOIs)

The following presents the **low level details of the "Credential-based access authorization through a terminal or via a portable device"** case, described in section 2.1: Operational Models. Specifically, this operation is split into two Use Cases, a and b:

I. Verifiable Credential Presentation: The Subject interacts with a terminal scanner or a portable device, and transmits to the access-controlling Service Provider a Verifiable Credential Presentation proving the required properties to gain access (Use Case a).

II. Derivative Credential Presentation: The Subject first interacts with an intermediary VC Transformation Service and generates a Derivative (or contextual) Credential, i.e. a short-lived

credential) and then presents that to a terminal scanner/portable device to gain access (Use Case b).

3.3.1 Verifiable Credential Presentation (Use Case a)

The process flow is defined as follows:

1. The Controlling Terminal Scanner or Portable Device displays a QR code containing a Verifiable Credential Disclosure Request
2. The Subject scans the QR code with their wallet app
3. The Subject's wallet reads the attributes contained within the Credential Disclosure Request
4. The Subject's wallet generates a new Pairwise DID to interact with the Service Provider that generated the QR code
5. The Subject's wallet prepares an appropriate Verifiable Presentation (VP), using ZK-proofs, from the available VCs stored in the subjects wallet
6. The Subject's wallet transmits the VP to the backend system of the Access Control Service Provider, using the metadata available in the Disclosure Request
7. The backend of the Controlling Service Provider, validates the VP and pushes the result to the Terminal Scanner, or Portable Device
8. The Subject is granted (or denied) access accordingly.

3.3.2 Derivative Credential Presentation (Use Case b)

The process flow is defined as follows:

1. The Controlling Terminal Scanner or Portable Device transmits via a Bluetooth Beacon[69] and through the BLE protocol, an appropriate verification request, denoting the area under control and the appropriate VC Transformation Service URI
2. The Subjects walle receives the transformation request and prompts the user to access the VC Transformation Service
3. The Subjects wallet receives a Verifiable Credential Disclosure Request from the VC Transformation Service
4. The Subject's wallet reads the attributes contained within the Credential Disclosure Request
5. The Subject's wallet generates a new Pairwise DID to interact with the VC Transformation Service
6. The Subject's wallet prepares an appropriate Verifiable Presentation (VP), using ZK-proofs, from the available VCs stored in the subjects wallet

[69] A Bluetooth Beacon is a hardware transmitter, a Bluetooth low energy (LE) device that broadcasts its identifier to nearby portable electronic devices. Once connected, smartphones, tablets and other mobile devices can "dialog" with a beacon when in close proximity to it.

7. The Subject's wallet transmits the VP to the VC Transformation Service, using the metadata available in the Credential Disclosure Request
8. The VC Transformation Service validates the VP, and responds by pushing to the users wallet a Derivative Credential
9. The Subject's wallet receives the Derivative Credential and presents it in a suitable manner (e.g. QR code or BLE beacon/BLE advertising packets)
10. The Subject scans the Terminal Scanner or Portable Device with the QR code, or transmits a BLE beacon
11. The Terminal Scanner or Portable Device reads the QR code, or process the BLE beacon, and contacts the VC Transformation Service to validate the Derivative Credential contained in the QR code
12. The Terminal Scanner or Portable Device grants (denies) access accordingly.

3.4 Document verification in ad hoc outdoor and indoor settings (DYOIs)

The following presents the **low level details of the "Digital Document Verification in ad hoc indoor and outdoor settings" case,** described in section 2.1 (Operational Models). Specifically, we assume that a **Subject receives "service interaction triggers" when entering a geographical area, more precisely a geofence**, i.e.. a virtual perimeter designed by a control officer to denote a real geographical area around a checkpoint, where a control process should take place[70] (the custom definition of virtual borders for such areas of control might be also carried out remotely by authorized health or public order officers). This is made possible through a web or a mobile interface, and with the use of geofencing techniques which allow for the custom creatii of Geofence objects (e.g., geo polygons) in an enterprise GIS enabled infrastructure.

More precisely, the process flow is defined as follows:

1. The Subject's Wallet receives a verification request by the authority (public or private) operating a process of document verification, upon entering a specific controlled area. The notification includes the zone's metadata, as well as the type of credential that is needed to be presented to the control officer, and might arrive via a mobile push notification from the mobile network, via a Beacon ID, or a BLE Beacon packet as the result of the user scanning a QR code that is placed on a visible spot within the controlled area. Since the requested Verifiable Credential should be ultimately verified by the mobile phone of the control officer, its transformation to a Derivative (Contextual) Credential is necessary (i.e. to a short-living token or to a seed phrase/word). Consequently, the received notification message must also include a pointer (URI) to the appropriate VC Transformation Service.

[70] See above: section 2.2.3

2. The Subject is prompted to access the VC Transformation Service where they consent to the Presentation of the requested Verifiable Credential following the process described above, in section 3.3.2: Derivative Credential Presentation (case b) - steps 3 to 8.
3. The VC Transformation Service validates the received VC presentation and responds by sending the corresponding Derivative Credential to the Subject's Wallet, and a validating key (paired with the Derivative Credential) to the control officer's mobile phone (via the back end of the Control Service Provider where the control office is affiliated). The Derivative Credential (DC) may be an encrypted short-lived token that automatically translates to a simple word made out from a seed phrase (different for every Subject).
4. The Subject's Wallet receives the Derivative Credential (DC) and broadcasts it, via BLE, to all nearby devices but only the mobile phone of the control officer can decrypt the received token; alternatively, the subject has only to memorize the received word which has trancoded an existing Verifiable Credential (their mobile phone displays also the received word on a green full screen background using white large fonts)[71].
5. The Controlling Device which receives and decrypts the DC (short-lived) token, validates it against the previously received validating key; alternatively, the Subject presents to the control officer the received word (verbally or by showing their screen).
6. If the mobile device can match the received DC token with the validating key, the control officer grants access to the Subject (or denies it in the opposite case); in a similar way, the control officer has already received in their mobile phone the same word that the VC transformation Service had forwarded to the Subject (as the instantiation of a Derivative Credential) and, if the Subject presents the right word, is granted access.

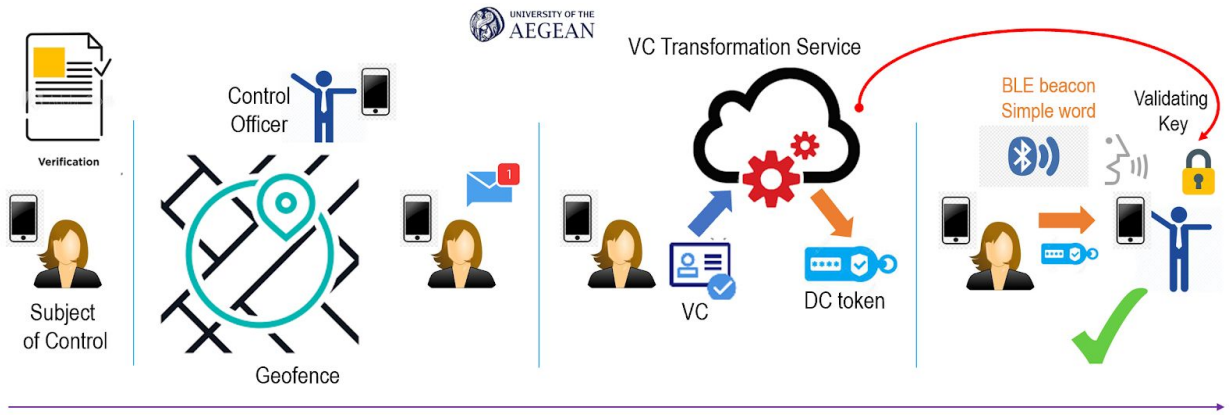

Figure 11: Digital Document Verification in ad hoc indoor and outdoor settings - Granular view

[71] The Subject may decide which of these two options to use, forward the received token via bluetooth or present the corresponding word. In other settings, the requirement of following one or the other option may be explicitly imposed by the control officer on the basis of the specific context of control.

One last point on the **connectionless session established between the two devices**. This is established with the use of a specific **bluetooth communication service** that we have designed for the needs of the (generic) case where two mobile devices must directly exchange a minimum data set. We should remind ourselves that the data packet used by the bluetooth protocol for broadcast is called a beacon packet (or a BLE advertising packet) and, according to the BLE specification, it can have a maximum data payload of 31 bytes[72]. From this data payload however, **only the 2 bytes "Major value" data field can be used as a "data store"**, that can supposedly take over the transfer of binary data from one mobile phone to another. We can therefore define, on the basis of this elementary data chunk, a **"stop and wait" communication service by applying a specific bit mapping technique** to the customizable data fields of a BLE beacon, thus making it able to serve as a data transfer facility between two mobile devices.

Essentially, we model this service as a "stop and wait" **application layer data transfer protocol** having:

- A standard BLE broadcast data packet with a static UUID value in the 16 bytes packet's Bluetooth Identifier, which informs the receiver that this broadcast packet serves as a packet for binary data transfer between the two devices.
- An ACK (acknowledgement) broadcast packet with a specific static UUID value in the Bluetooth Identifier, different from those of the standard binary data transfer BLE packet, which alerts the sender that this broadcast packet is in fact the acknowledgment packet of a previous successful data packet broadcast.
- The 2 bytes "Major value" field of the standard broadcast packet is the basic transfer unit of the designed service, while the 2 bytes of the "Minor value" data field is used to denote a Session (Ephemeral) Identifier and a Sequence Number to identify broadcast packets ordering.
- A bit mapping blueprint to implement the basic flow control mechanism for the connectionless data transfer protocol. The 2 bytes of the "Major value" field are populated with an integer number; it has the same bit mapping as the 2 bytes encrypted data chunk,, stored inside every single BLE broadcast packet. Similarly, the 2 bytes of the "Minor value" field are populated with an integer number; its binary representation contains a unique random Session Identifier in the first eight (8) bits, and the Sequence Number of each session packet in the last eight (8) bits[73].
- Respectively, an ACK (acknowledgement) BLE broadcast packet shares the same Major and Minor fields integer values with the BLE broadcast data packet of which reception is acknowledged.

From a **performance** point of view, our proposal allows for the transfer of a Derivative Credential (DC) of a maximum size of 512 bytes (with 1 byte reserved to each data packet sequence number, and 2^8 maximum sequence numbers, we can transmit a maximum of 256 broadcast packets per data transfer

[72] See above: section 2.2.2.3

[73] Due to BLE SDK programming limitations, only integer values can be set to the Major and Minor values fields of a BLE advertising packet.

session; given that each packet carries 2 bytes of data, we have 512 bytes, i.e., 2x256, which is the maximum capacity available to the transmission of an encrypted Derivative VC. The transmission time ranges between 11,4 milliseconds (for a 2 bytes DC) to 2.9 seconds (for a 512 bytes DC), assuming that there is a random 0 to 10 millisecond additional delay added per transmission (this prevents two BLE devices with the same advertising interval from being stuck transmitting at exactly the same time forever and possibly interfering with each other).

However, in a crowded environment simultaneous BLE wireless broadcasts from mobile devices lead to packet collisions. Our proposed (**"stop and wait") application layer data transfer protocol** includes a countdown timer when it waits to receive an ACK packet for a previous data packet broadcast. If the timer ends before the reception of the ACK packet, the data packet is considered lost (eventually as the result of a collision with another broadcast in the wireless medium) and the protocol proceeds to a retransmission. The delay time before a new data packet transmission occurs is varying and depends entirely on the specific (exponential) **backoff algorithm** that is used. In simple terms, in the case of repetitive losses of ACK packets, the random delay time before transmission increases by small random increments, to reduce the possibility of a packet collision due to a simultaneous transmission from another nearby mobile device.

4. Epilogue

The theoretical underpinning of Disposable Identities has been formed in the Identity workshops in the Next Generation Internet Strategy Team NGI Forward[74]. COVID-19 has amplified the conceptual drivers that underlie privacy and security in processes of identity verification.. **Three main scopes of interest inform its current uptake**[75].

The first is the **Internet of Things and the emerging hybrid cyber-physical world.** In a hybrid world connected artefacts respond to and actuate in real time with real time data streams originating in automated information systems. And the outbreak of COVID-19 is proving to be a catalyst for a fast emerging **"touchless economy"** which is a new trajectory[76] of automation. Organizations will need to re-design their operations and transform to meet the needs of the touchless modes of access and process management.

The second is a political argument. Decentralized identities are going to replace usernames and passwords and other forms of existing eIDs with IDs that are self-managed and use Distributed Ledger Technologies (DLTs) and other complementary innovations to establish "collective trust" and protect privacy. By

[74] See in particular, NGI Forward, 2020. D4.7 Innovation Summit Report, mimeo

[75] See also: https://www.disposableidentities.eu/about-disposable-identities-community-statement

[76] In the sense of G. Dosi, 1982, Technological paradigms and technological trajectories: A suggested interpretation of the determinants and directions of technical change, available at https://www.sciencedirect.com/science/article/abs/pii/0048733382900166

definition, decentralized Identities establish the principle of minimal data processing (i.e., the amount of identity data processed should be adequate but limited to what is necessary for the identification purposes). Disposable Identities, a specific form of decentralized identities which allow users to issue and use contextual but authoritative identities, may be a response to growing people's fears of privacy-invasion. As privacy increasingly becomes a very societal issue, **disposable Identities can create an opportunity for a "technical accommodation" of the "tussle"[77] between competing views on privacy and paralyzing conflicting interests** between governments, large tech corporations. NGO defending civil liberties, influencers, aficionados of decentralization etc. (as the recent case of COVID-19 contact-tracing apps has perfectly demonstrated).

The third is that we are part of a growing movement that is happening: the current debate on Self-Sovereign Identities (SS) is moving into the mainstream (as part of a more generic innovation wave promoting self-sovereign technologies[78] It is clear that we need identity custodians, as people are not educated into handling private keys. Custodians are the key to SSI success. **Identity Management Custodians should be the cornerstone of a governance model for SSI implementations that still need to be discovered**.

[end of paper/Sept2020]

[77] In the sense of D. Clark, 2002, Tussle in Cyberspace: Defining Tomorrow's Internet, available at https://david.choffnes.com/classes/cs4700fa14/papers/tussle.pdf

[78] In this regard, see in particular: https://docs.google.com/document/d/1kZ7_Skcn4zb3zOfEu7XZDrYAmLR1T_pbBoSk8AEfrSg/edit