



RiBAC: Strengthening Access Control Systems for Pandemic Risk Reduction while Preserving Privacy

Stephan Krenn

stephan.krenn@ait.ac.at

AIT Austrian Institute of Technology
Vienna, Austria

Daniel Slamanig

daniel.slamanig@ait.ac.at

AIT Austrian Institute of Technology
Vienna, Austria

Jan Orlicky

jan.orlicky@ima.cz

IMA s.r.o.
Prague, Czech Republic

Tomáš Trpišovský

tomas.trpisovsky@ima.cz

IMA s.r.o.
Prague, Czech Republic

ABSTRACT

Traditional (physical) access control systems are well-established mechanisms, allowing organizations to determine who should be able to access which physical space. This can either be a facility such as a critical infrastructure with a well-defined set of individuals, e.g., employees, or public spaces where everyone can be subject to access control. During the Covid-19 pandemic, additional features to reduce the risks of individuals when entering spaces became popular or even mandatory, including automatic scanning for protective wear (e.g., whether an individual wears a mask), body temperature checks, or digital health certificates, certifying that one has been negatively tested for, or vaccinated against, Covid-19. We refer to this as risk-based access control (RiBAC).

In the Covid-19 pandemic largely due to the time pressure for implementing these measures, many of such RiBAC extensions to classical AC systems required manual intervention. This, besides posing health risks for the individuals performing these checks, yields a solution which is not scalable. Now that the Covid-19 pandemic no longer constitutes a public health emergency of international concern by the World Health Organization (WHO), it is time to reconsider RiBAC systems. Our main focus in this work is to investigate requirements for such systems and to discuss possible generic architectures for RiBAC systems. In order to be prepared for a future pandemic, the goal should be to implement such systems in a way such that they are scalable and risk-minimizing. We will specifically focus on privacy of the individuals subject to access control in RiBAC, while preserving the functionality of the system. Moreover, our focus is on the European setting where digital health certificates were considered as a central risk-reducing mechanism. In this context, we discuss the use of privacy-preserving cryptography in order to be able to have RiBAC systems that are privacy-preserving already in place for any potential future pandemic.

KEYWORDS

Physical access control, risk-based access control, privacy, privacy-preserving cryptography

ACM Reference Format:

Stephan Krenn, Jan Orlicky, Daniel Slamanig, and Tomáš Trpišovský. 2023. RiBAC: Strengthening Access Control Systems for Pandemic Risk Reduction while Preserving Privacy. In *The 18th International Conference on Availability, Reliability and Security (ARES 2023)*, August 29–September 01, 2023, Benevento, Italy. ACM, New York, NY, USA, 9 pages. <https://doi.org/10.1145/3600160.3605039>

1 INTRODUCTION

Physical access control (AC) systems enable organizations to restrict access of single users or groups thereof to physical spaces. In their most basic form, such AC systems consist of doors, locks, and keys – however, modern access control systems go far beyond this, and include advanced access credentials, e.g., including key cards, smart phone credentials, encrypted badges, and biometric-based validation of a user’s identity, allowing for fine-grained access rights to different facilities. The reasons for using advanced access control mechanisms are multi-fold, ranging from the protection of assets such as facilities, equipment, or technologies, over the tracking of visitors and employees to detect suspicious behaviour, e.g., due to a lost or stolen access card, up the protection of employees by ensuring that no unauthorized persons may enter a building.

Complementary to these goals, an additional type of access control has emerged over the last years, which we refer to as *risk-based access control* (RiBAC).¹ The goal of this type of access control is not so much to ensure that only eligible persons may enter a space, but rather to guarantee that they are healthy, do not pose a health risk to others, or to ensure that workers of different shifts do not mix. Traditional measures, include, e.g., large-scale infrared thermal image scanners at airports during influenza seasons to ensure the healthiness of travellers. Furthermore, RiBAC has gained significant attention during the Covid-19 pandemic. Examples for implemented risk checks include automatic scanning for protective wear (e.g., whether an individual wears a mask), body temperature checks, asking a list of questions that can be used for vetting



This work is licensed under a Creative Commons Attribution International 4.0 License.

ARES 2023, August 29–September 01, 2023, Benevento, Italy

© 2023 Copyright held by the owner/author(s).

ACM ISBN 979-8-4007-0772-8/23/08.

<https://doi.org/10.1145/3600160.3605039>

¹We are aware of the fact that the term “risk-based access control” is already used for access control mechanisms where access decisions are based on quantified risk estimates [8]. Nevertheless, we believe that it also provides a good intuition for pandemic situations where we want to *reduce risk* via access control.

possible risks, and different types of digital health certificates [28] like the EU Digital COVID-19 Certificate², often also referred to as “green pass”. Latter certifies that one has been negatively tested for, or vaccinated against, Covid-19.

Especially during the Covid-19 pandemic, adding RiBAC features to existing AC systems as well as the design of the RiBAC components happened in an ad-hoc way. In the light of preparedness for future pandemics, a natural question that arises is how the integration of these two systems can or should be done. Moreover, most ad-hoc design substantially sacrificed the privacy of users. The emerging issues have been studied and analyzed in a series of papers [18, 24] and appropriate recommendations for the correct implementation of vaccine passports have been made. Consequently, now is the time to revisit RiBAC designs with a particular focus on user privacy.

However, combining RiBAC with existing AC mechanisms poses a variety of challenges. For instance, digital health certificates (such as the above mentioned “green pass”) are usually designed in a way that requires the manual verification of a user’s identity, i.e., they have not been designed with an automatic access control mechanism in mind. However, without this manual identification it cannot be ensured that the certificate indeed belongs to the individual, making the process an efficiency bottleneck in many scenarios. Moreover, as in case of Covid-19 representing a contagious disease such manual checks increase the risk of exposure and contactless solutions are highly desired. Another challenge is the privacy of users³: while in combination with traditional access control, e.g., to critical infrastructures, the identification of users will be required, it is still necessary to protect a user’s privacy in terms of the health status (e.g., tested or vaccinated), as long as the underlying access policy of RiBAC, e.g., the user must either be vaccinated within the latest 6 month or tested negatively within the last 24 hours, is satisfied. Even worse, in the case of access to public places such as restaurants or public transport, already the identification of the user may be unacceptable, and the RiBAC system needs to work on a fully anonymous level. Finally, the integration costs with existing solutions needs to be kept as low as possible, while the efficiency of the solution needs to be sufficiently high, also for heavily frequented places.

1.1 Related Work

During the Covid-19 pandemic, a variety of digital solutions to minimize infection risks were developed.

For instance, one very popular, but highly debated, solution were digital contact tracing (DCT) solutions [26]. Out of a multitude of protocols, e.g., [19, 21, 25, 27], the most well-known is the Decentralized Privacy-Preserving Proximity Tracing (DP-3T) protocol [27] relying on Bluetooth Low Energy (BLE), which also heavily influenced the Google and Apple Exposure Notification (GAEN) framework [14] used by most DCT apps. We will not discuss DCT solutions in more detail here, as they can be viewed orthogonal to the RiBAC setting that we have in mind.

²https://commission.europa.eu/strategy-and-policy/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en

³<https://www.forbes.com/sites/hessiejones/2021/02/19/can-verifiable-credentials-be-the-key-to-safely-reopening-the-economy/>

Frederiksen [11] investigates security and privacy issues in digital health certificate (DHC) applications and then demonstrates a solution based on a distributed password-based authentication protocol [2] with improved untraceability by replacing distributed signatures by blind signatures [6] (another important privacy-enhancing technology). While the former work solely focuses on digital credentials, Hicks et al. explore various design ideas for decentralised, privacy-preserving DHC protocols [17] that allows for both paper-based and app-based user credentials.

Godden et al. investigate privacy-preserving variants of the EU Digital COVID Certificate [13] and in particular use a toolchain for zero-knowledge proofs that works with the Belgian EUDCC.

Binding digital certificates and credentials to humans has been an active field of research over many years. For instance, Adams et al. [1, 12] consider binding of credentials to individuals through biometrics. The case of Covid-certificates has recently also been analyzed by Hesse et al. [16].

Finally, we want to mention that the deployment of DHCs has inspired the design of various distributed systems with a particular focus on self-sovereign identity (SSI) as well as distributed ledger technologies [9].

1.2 Outline

In Section 2, we introduce the main components of risk-based access control mechanisms, describe motivating application scenarios, and elicit some fundamental requirements to such systems. Then, in Section 3 we describe three generic architectures for RiBAC systems with different levels of integration with the underlying access control mechanism, and discuss their suitability for the motivating scenarios and how they address the specified requirements. Finally, we briefly conclude and discuss open challenges in Section 4.

2 SCENARIOS AND REQUIREMENTS

In a RiBAC system, *individuals* wish to access a area protected by an access control (AC) system. We refer to the traditional, non risk-aware part of the system which may already be in place, as the *classical AC system*. Such a system is enhanced by *RiBAC extensions*, which are responsible for any risk-related aspects. Such an add-on may be based on physical checks (thermoscans, etc.), or leverage certificates such as *digital health certificates* (DHC) attesting certain attributes. The requirements that an individual has to fulfill in order to be granted access by the RiBAC extensions are specified in an *access policy*; for instance, such a policy could require that a person is wearing a face mask, and in addition was negatively tested in the past 48 hours or vaccinated twice in the last 6 months. Finally, together, the classical AC system and the RiBAC extensions form the full *risk-based access control system*.

In the following we now briefly discuss possible application scenarios for RiBAC systems, and perform a high-level requirements analysis for such systems.

2.1 Application Scenarios

In the remainder of this paper, we will mainly be guided by two complementary use cases for risk-based access control, which we will briefly outline in the following.

Critical infrastructure access control. As a first motivating use case, we will consider access control to critical infrastructures, as well as other access-restricted areas such as, e.g., work facilities, where strong classical access control mechanisms are typically already in place. In such a scenario, RiBAC extensions are needed to protect the work force, which is particularly required to ensure the proper functioning of critical infrastructures during pandemics.

Typically, the classical AC system will uniquely identify each individual when entering the area, e.g., by scanning employee badges or similar. It is therefore necessary to ensure that the RiBAC extensions refer to the same individual, and do not leak any additional sensitive information (e.g., the vaccination status). However, anonymity within the overall RiBAC system is not a requirement, and the RiBAC extensions may potentially refer to the identity coming from the classical AC system.

Access control for public spaces. Orthogonal to the above use case, our second application scenario is access control to public spaces such as public transport, shopping malls, or theaters. For instance during the Covid-19 pandemic, access to such public spaces was subject to certain restrictions (e.g., negative test result, etc.) in various countries. In this case, no classical AC systems are in place, which can be used to verify the identity of a certificate holder. For this reason, as described above, manual steps in the validation process were needed, posing a scalability bottleneck and causing increased personnel costs.

Even more challenging, the anonymity of individuals should be protected to the maximum degree possible and no identification should occur. Only in exceptional cases identification might be required at a later point, e.g., it is known that an infected individual was present at a certain time and other individuals who were there close in time need to be identified and notified.

2.2 Requirements

For requirements elicitation we leave the **effectiveness** of certain checks out of scope, as these cannot be addressed on a technical level, but need to be designed and validated on a medical or epidemiological level. Furthermore, we here do not state obvious requirements, e.g., relating to **accuracy** (i.e., low false-negative and false-positive rates) or **usability**, as those also do not directly impact the integration of RiBAC extensions into classical AC systems, but need to be validated independently.

The first three requirements specific to RiBAC extensions are now related to security and privacy:

Security. From a security perspective, it is of utmost importance that an access control system extended by risk-based features is no less secure than the underlying classical AC system. In particular, it must not be possible for a malicious individual to leverage the extension to gain access to resources that they would not have been granted access to by the original AC mechanism.

Privacy. A RiBAC scheme should fully respect the user’s privacy, and not leak more information than the underlying classical AC system and beyond what is revealed by the access policy itself.

For instance, if the classical AC system uniquely identifies a user, the RiBAC system must not disclose any additional information such as, e.g., the vaccination or recovery status. Contrary, if the underlying classical AC system does not require the identification of the individual, also the RiBAC system must not reveal the identity or any other uniquely identifying attributes of the individual for authentication purposes, but rely on appropriate privacy-enhancing technologies.

Unlinkability. In particular in scenarios where an identification of an individual is not necessary, it should additionally be guaranteed that different actions of the same individual cannot be linked, as otherwise tracking of individuals would become possible, potentially disclosing sensitive meta-information. This unlinkability should hold against all entities in the RiBAC ecosystem, in particular including issuers of DHCs as well as verifiers.

The following requirements are mainly related to practical aspects regarding efficiency as well as feasibility and costs of real-world deployments:

Hardware requirements. The hardware requirements on the user side should be kept at a minimum level, depending on the specific application scenario. For instance, while in restricted work areas dedicated hardware tokens (e.g., additional smart cards) might be acceptable, large-scale solutions for public spaces should at most require access to a commodity device such as a smart phone.

Scalability. In order to achieve scalability, a RiBAC system should be fully automated, without human involvement in the verification of access policies. Furthermore, the throughput of the system should not be significantly less than that of the underlying AC system. Finally, while scalability can often be achieved by increased computational resources, the computational costs on the user’s and verifier’s side should be kept as low as possible.

Integrability. The costs and complexity of integration of risk-based extensions into existing AC systems should be kept as low as possible. This covers aspects regarding the actual deployment complexity, as well as the administrative complexity, e.g., of issuing dedicated hardware to all users or similar.

Interoperability. To minimize the overhead and increase acceptability of a RiBAC solution, it needs to be as interoperable with existing infrastructures and architectures as possible. For instance, in the case of infectious diseases in the European Union, a solution should be able to leverage digital EU Digital COVID Certificates without requiring issuers to adapt their processes and data flows. Likewise, when requiring to verify a user’s identity, existing standards such as the European Digital Identity⁴ need to be followed.

The final two core requirements identified for RiBAC systems are related to their epidemiological impact:

⁴https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en

Risk preservation. A RiBAC system needs to be risk-preserving in order to guarantee safety. That is, no additional health-related risks for the user must be introduced by the RiBAC features of the system. For instance, in the case of protection against infectious diseases, this means that a RiBAC system must be fully contact-less, in the sense that it neither requires additional personal interaction nor touching sensors or surfaces.

Tracing support. In case that a suspected or proven case occurs within the access-restricted area, it should be possible to notify individuals that have entered the area within a certain time interval to support public health authorities in fighting the spread of the pandemic. This needs to happen in a fully transparent way minimizing the privacy impact for the individual user, in particular avoiding full de-anonymization if possible.

2.3 Required Concepts

In the following we briefly discuss some concepts that are essential to the understanding of the RiBAC architectures discussed in this work.

EU DCC Digital Health Certificates. During the Covid-19 pandemic, the European Union chose to deploy the EU Digital COVID Certificates (EU DCC) as a risk mitigation measure. It represents a type of DHC and such systems based upon an open source implementation⁵ have been in use in all EU Member States, European Economic Area (EEA) countries as well as many countries outside the European Union⁶. Recently, also the World Health Organization (WHO) announced that it will take up the EU DCC to protect against future pandemic events.⁷

Conceptually, it employs digital signatures issued by a national authority to sign a document binding identifying information of an individual (name, date of birth, etc.) to their status, i.e., vaccinated, recovered, or tested. The status also includes additional attributes such as the type of vaccine or the date of vaccination, recovery, or test. Verification is performed locally and offline. The standard setting requires the user to run an app on the smartphone, which downloads and stores the signed document. For the actual check it displays a QR-code including the document and its signature. This QR-code is scanned by the verifier, the signature is verified and this is followed by a manual check. This includes checking the personal attributes against a physical identity document of the individual, e.g., a passport or driving license.

Attribute-based anonymous credentials. Attribute-based anonymous credentials (or ABCs), first envisioned by Chaum [5, 7] and later instantiated in a large body of work starting with Camenisch and Lysyanskaya [4], allow users to receive digital credentials certifying pieces of information or attributes, e.g., name, date of birth, etc., from an issuer. Later, users can decide to selectively present parts of this information (e.g., name) to a verifier, while keeping other parts (e.g., date of birth) secret. At the same time,

the verifier receives provable cryptographic guarantees about the authenticity of the disclosed information. Even more, in advanced schemes users can prove predicates over their attributes instead of fully revealing them (e.g., “older than 18” instead of the date of birth). Finally, ABC systems usually guarantee unlinkability, making it impossible to link two presentations.

3 GENERIC ARCHITECTURES

In this section we discuss three generic architectures for designing RiBAC systems, as well as non-trivial requirement considerations. These architectures can largely be classified by how deep the additional RiBAC features are integrated into the classical AC system. Thereby, we start from settings where classical AC systems are already in place and are extended by RiBAC features to RiBAC systems that are designed from scratch. In our consideration we omit the simplest approach, which just deploys RiBAC features but is not connected to any AC system and does not require any form of digitalization, e.g., temperature screenings on airports.

While the architectures presented in Sections 3.1 and 3.2 are mainly suited for situations where strong access control mechanisms are already in place (e.g., work places, critical infrastructures), the approach described in Section 3.3 rather focuses on public spaces (e.g., restaurants, shopping malls) where no classical AC is required.

3.1 Parallel Architecture

The first and arguably simplest architecture, illustrated in Fig. 1, composes a classical AC system and the RiBAC components in *parallel*. Thereby, both systems are completely disconnected, perform their decisions independently in parallel, and do not exchange any information. Clearly, this disconnection requires the components to be in close proximity to ensure that only one individual at the time is subject to access control, so that it can be guaranteed that both decisions are with respect to the same individual.

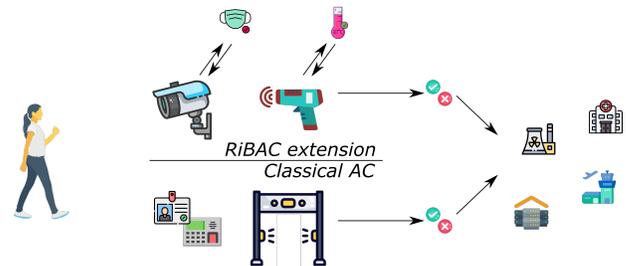


Figure 1: Parallel architecture

Advantages. The main advantage of this parallel architecture is that it is easy to deploy and does not require modifications to the classical AC system or an existing solution realizing the RiBAC features. It is an attractive solution when the RiBAC features only focus on physical checks (e.g., body temperature, presence of protective measures such as a face mask), i.e., features that are not specific to the identity of the individual and do not require digital certificates attesting attributes of the individual beyond those that can be easily determined by sensors. Moreover, if the underlying components provide scalability, then the overall system will provide

⁵<https://github.com/eu-digital-green-certificates>

⁶https://health.ec.europa.eu/ehealth-digital-health-and-care/ehealth-and-covid-19_en

⁷https://commission.europa.eu/strategy-and-policy/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en

scalability. Same holds for being risk-preserving, e.g., if the single components are contactless and do not provide human intervention, so will the composed system.

Consequently, it is not surprising that for many countries in beginning of the Covid-19 pandemic this has been the prevalent architecture.

Disadvantages. The main disadvantage stems from the disconnection of the two systems. If the RiBAC components need to base their decisions on information that goes beyond physical checks, e.g., information from a digital health certificate (DHC) of the individual, then there is no link between the two systems. Consequently, without additional measures individuals could maliciously use such information from other individuals, e.g., a DHC from someone else. While such problems can be prevented by manual intervention, e.g., a human check guaranteeing the match of the identity of the individual and that of the DHC, such manual checks negatively impact scalability and are not risk-preserving. One measure to overcome these limitations is to add a biometric layer (cf. [12]) which matches biometrics of the individual to biometrics encoded in the DHC. This however increases the deployment costs and might contradict the benefits of the parallel architecture.

3.2 Sequential Architecture

The second architecture, illustrated in Fig. 2, composes a classical AC system and the RiBAC components *sequentially*. In this context, we assume that the RiBAC components involve checking attributes of the individual that are linked to their identity, e.g., an access policy that needs to be satisfied by the DHC. Consequently, in addition to the access decision, the classical AC system outputs some information *ID* that can be used as an input to the RiBAC components to link the identity of the individual in the former system to the latter components. Here, *ID* can either be an external identifier that is used, e.g., by the DHC, or it can also be a combination of attributes, e.g., name, date of birth, of the individual that are used by the classical AC as well as the RiBAC components.

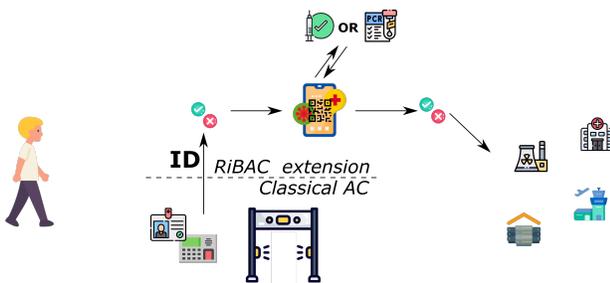


Figure 2: Sequential architecture

Online- vs Offline RiBAC verification. The architecture in Fig. 2 is agnostic to whether the RiBAC verification is taken locally or online. More precisely, the verification by the RiBAC components and in particular the DHC could be performed offline, e.g., co-located with the classical AC system, or deferred to some on-line entity. For instance, assuming that there is a national infrastructure in place that keeps track of the vaccination status and Covid-19 test

status of all citizens, the RiBAC component could just outsource the decision for the access policy to a service provided by the national infrastructure, basically by sending the *ID* and just processing the result, representing a yes or no decision.

Online verification may have advantages in terms of accuracy: for instance, if a vaccinated individual receives a positive test result, they could still use the vaccination certificate to enter a facility if no online verification of the status is carried out, because no (temporary) revocation of vaccination certificates can be enforced. On the downside, however, an online process poses challenges regarding the individual’s privacy and unlinkability:

- Firstly, the central authority may learn when an individual wishes to enter which facility. In case of restrictive access rules at many places, this could enable the authority to derive a detailed movement profile of citizens. It is thus important that the verifier does not authenticate itself towards the authority. In this case, only the number and timestamp of an authentication is revealed, but no tracing of the individual becomes possible.
- Secondly, a malicious verifier could send periodic requests about the health status of a target individual to the authority to learn about possible infections or whether they have been vaccinated or not. It is thus important to enforce the physical presence of the individual upon such a request. This can, e.g., be achieved by letting the individual digitally sign a timestamp and *ID*, which is sent to the authority together with the *ID*; if the timestamp is not fresh, the request would be denied. However, in this case it is required to keep track of the public verification keys of all individuals. This leads to a key management challenge, unless a national electronic identity (eID) solution can be leveraged.
- Finally, online verification has the disadvantage that in case of an outage of the central authority all RiBAC systems would be affected and become inactive.

It is worth noting that the current EUDCC is offline, also because no central database of test results exists in certain countries, and also cross-country interoperability would be challenging (e.g., individuals from country A being tested in country B and travelling to country C).

Paper-based vs digital health credentials. During the Covid-19 pandemics, health credentials have often been issued also in paper-based form for various reasons, including convenience and avoidance of discrimination of users without a smart phone. However, we want to note that paper-based health credentials come with some inherent limitations. Firstly, a static QR-code as was displayed, e.g., on Covid-19 vaccination certificates, necessarily makes users fully linkable. Secondly, and more importantly, also privacy cannot be achieved with such certificates, as individuals cannot dynamically prove that they satisfy given access policies (e.g., vaccinated or tested) at a given point in time.

These limitations cannot easily be addressed by mitigation strategies like not encoding the vaccination status but only the expiration date of the vaccination credential, and letting the verifier check that this date has not yet passed: besides giving up on flexibility in case of different access rules for different types of places, while the vaccination status is not explicitly revealed, it could easily be

inferred if the expiration date is more than 48 hours in the future. We therefore consider digital health certificates to be indispensable for the design of usable solutions with high privacy guarantees.

Advantages. The main advantage over the parallel architecture from Section 3.1 is that *ID* allows one to connect the two systems, and guarantees (depending on the uniqueness of *ID*) that both access control decisions are performed with respect to the same individual. In applications such as access to work facilities, where anonymity of the individual is not important, but only specific attributes (e.g., vaccination status) shall be kept private, this architecture seems most reasonable. In particular, in such settings a simple combination of attributes will already make *ID* unique with high probability. Note that it cannot be formally guaranteed that a DHC belongs to the individual on which the classical AC system performs the access decision without additional means, e.g., manual check of the identity, if using a DHC in the parallel architecture.

Disadvantages. A disadvantage compared to the parallel architecture is that this architecture requires changes to the existing classical AC system. Nevertheless, these changes can be considered relatively minor as it simply amounts to providing the output of some information available in the classical AC system in a way accessible to the RiBAC components. One issue that can become challenging is that when using this architecture in a privacy-preserving way across different domains, it might be necessary to consider different identifiers for the different classical AC systems within the RiBAC components, e.g., DHCs cannot include external identifiers for multiple traditional AC systems.

Interoperability challenges. In contrast to the parallel architecture from Section 3.1, by connecting two systems and introducing additional features bound to the identity of the individual for the RiBAC component, e.g., using a DHC, this introduces interoperability challenges. This gets particularly evident when aiming for strong privacy features. As mentioned above, connecting the two systems via a simple but likely unique *ID*, e.g., name, date of birth, that is also available in the DHC, allows a simple connection of the two systems and does not require any changes to the DHC system. However, when relying on existing solutions for DHC such as the EUDCC, representing an offline and local system, it does not represent a privacy-friendly solution. In particular, the whole DHC is transferred to the verifier and it discloses much more information compared to only learning whether the policy is satisfied or not.

In order to support stronger privacy guarantees for the DHC component, changes have to be introduced to the system, such as a replacement of the conventional digital signatures with attribute-based anonymous credentials as discussed in Section 3.3. However, this requires a complete redesign of the DHC solution and modification to issuers of the certificates, the user app as well as the verifier. Another possible solution is to still rely on DHC, but to change the user app and verifier side to integrate privacy features. From a technical perspective, there are different ways to realize such a feature. In particular, one can rely on intermediate certification either using concepts from self-sovereign identity and verifiable claims relying on zero-knowledge proofs⁸ or anonymous credential

systems that are specifically designed to deal with existing identity infrastructures [22].

3.3 By Design Architecture

The third generic approach, illustrated in Fig. 3, fully integrates the RiBAC extensions into the access control mechanism. In this setting one can also follow a strict privacy-by-design approach, which is only possible in a limited way for the two other approaches. In particular, this last architecture is also suitable for scenarios like access control to public spaces without violating the privacy of the user.

In a nutshell, the idea of the approach is as follows: the individual receives a digital credential, e.g., in form of an attribute-based anonymous credential [4], certifying, among others, the health status, some biometric features, and the identity of the individual. Then, for risk-based access control, the user selectively discloses the information that is needed to fulfil the access policy (e.g., vaccinated or negatively tested), and in addition proves that they own the biometric features encoded in the credential. Given the sensitivity of biometric information, and in order to fully maintain privacy, all these checks need to be carried out in the encrypted domain, e.g., using efficient (non-interactive) zero-knowledge proofs of knowledge [10, 23] or zk-SNARKs (succinct non-interactive arguments of knowledge) [15]. Binding the credential to the physical identity of the individual prevents from sharing of certificates, while the deployed privacy-enhancing technologies guarantee privacy.

A detailed formalization of this approach has recently been proposed by García Rodríguez et al. [12], specifically supporting face recognition as a biometric feature. In their setting, the biometric reader as the verifier has to be trusted in the sense that it never discloses biometric readings to the verifier in plaintext, but only in encrypted form. The user then locally computes a zero-knowledge proof that this encrypted biometric scan corresponds to the biometrics encoded in their credential. However, a minimum amount of trust seems to be unavoidable when aiming for non-transferability of credentials without introducing dedicated hardware. For an in-depth discussion, we refer to [12].

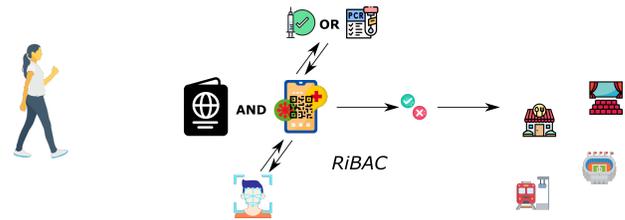


Figure 3: By-design architecture

While similar to Section 3.2 both online and offline verification could be supported, the following discussion mainly focuses on offline verification, as this is also the design choice that has been taken for the EUDCC. Still, all discussions from the previous section apply.

Advantages. The main advantage of this approach is the high level of privacy that can be achieved. By the guarantees of the deployed technologies, fully privacy-preserving access control across

⁸<https://www.w3.org/TR/vc-data-model-2.0/#zero-knowledge-proofs>

different domains is supported, ensuring that an individual cannot be identified at any point in time. Even more, also different activities and authentications of the same individual cannot be linked, such that tracing of individuals becomes impossible also for an adversary who controls multiple verifiers and the issuer. Furthermore, the full flexibility of attribute-based anonymous credentials and zero-knowledge proofs can be used, such that also complex predicates (e.g., “last tested at most 48 hours ago”) can be proven efficiently. Finally, by binding the credentials to physical properties of their owners, a high level of assurance is achieved, as credentials cannot be transferred among users, which is often not even achieved in classical AC systems using, e.g., key cards or similar.

Disadvantages. While the feasibility of this by-design approach has been shown, e.g., by García Rodríguez et al. [12], this approach is the computationally most expensive one. That is, while authentication can efficiently be performed on smart phones, an implementation on smart cards or similarly constraint devices currently seems to be out of reach, if transferability of credentials is to be avoided. Furthermore, the approaches from Sections 3.1 and 3.2 are relatively easier to integrate into classical AC systems, while the approach presented above requires a full re-design of the access control system, which however may be acceptable in cases where no classical AC system was in place before.

Tracing support. Considering the approaches from the previous sections it is relatively clear how to notify individuals in case they were exposed to an infectious person, as information about the entering individuals is handled by the classical AC system. However, the presented approach follows the privacy-by-design paradigm, achieving high provable privacy and unlinkability guarantees, making later notification of individuals difficult. One possible solution could be to integrate the so-called feature of inspection [3, 20]: in this case, an encrypted version of the individual’s identity is handed to the verifier, together with a cryptographic validity proof, under the public key, e.g., of the health authority. Now, in case that the authority needs to re-identify people, the verifier could hand over the encrypted identities of individuals entering during the period in question. This allows for a trade-off between full anonymity and the possibility to de-anonymize exactly those individuals that have potentially been exposed to a risk, as the ciphertexts remain with the verifier, and thus the authority (or an attacker gaining access to their key material) could not perform large-scale tracing of citizens.

Alternatively, instead of encrypting one’s identity, individuals could simply encrypt, e.g., a random string of sufficient length, which they also store locally. In case of a potential exposure, authorities could now obtain the ciphertexts, decrypt them, and publish the random strings. Users could then match the published values against their local data. While in this case authorities would no longer be able to re-identify citizens and, e.g., put them under quarantine, they would still be able to inform citizens about the exposure risk. This approach would be very similar to what has been done, e.g., by digital contact tracing solutions such as DP-3T [27] or GAEN [14].

Privacy and Unlinkability. Besides the biometric binding to avoid transferability of DHCs to achieve scalability and reduce personnel efforts, the presented approach also significantly varies from

the existing EUDCC approach in terms of unlinkability and privacy. Namely, in the EUDCC framework, all information contained in the DHC is transferred to the verifier, who then locally verifies the validity of the digital signature, which is followed by the manual verification of the identity. However, there is a discrepancy between what is revealed and what is required and used. While only the name and date of birth needed for identity verification as well as an indication whether or not the access policy is satisfied would be required (and are displayed to the verifier in the application), the application learns all information about a user (including, e.g., type and date of test or vaccination, etc.). We note that a verifier app could easily be modified to store all this data, posing a severe privacy risk. This is in contrast to the privacy-preserving approach presented here: while the same soundness guarantees regarding the health status of the individual are achieved, no further information is ever sent to the verifier, who rather only receives a cryptographic proof that the access policy is indeed satisfied.

4 EVALUATION AND OPEN CHALLENGES

In Table 1 we now evaluate the different approaches presented in this paper against the requirements set out in Section 2.2. Furthermore, the table contains the set of epidemiologic checks supported by the three architectures.

As can be seen, security and risk-preservation are fulfilled by all approaches. Furthermore, privacy can be fulfilled by all three approaches, in the case that privacy-preserving digital health certificates, e.g., allowing for selective disclosure, are deployed. In particular, as discussed earlier, privacy cannot be fully achieved using paper-based health certificates.

Unlinkability is a strong privacy requirement that is only meaningful when identification of the individual is not required, e.g., for access control to public spaces, and is thus typically not critical in cases where traditional AC systems are already in place.

	Architecture		
	Parallel	Sequential	By-design
Requirements			
Security	●	●	●
Privacy	●	◐	●
Unlinkability	○	○	●
Hardware requirements	●	●	◐
Scalability	●	●	◐
Integrability	●	◐	○
Interoperability	●	◐	○
Risk preservation	●	●	●
Tracing support	●	●	◐
Supported checks			
Physical (temperature, etc.)	●	●	●
Digital (DHCs)	○	●	●

Table 1: Evaluation of the different approaches relative to the requirements and overview of supported checks (●=fully satisfied, ◐=partially satisfied, ○=not satisfied).

For the remaining requirements, there exist trade-offs: while the by-design architecture (Section 3.3) offers the highest privacy guarantees, the complexity of deployment and integration, as well as interoperability with existing infrastructures, cannot be guaranteed. The possibility to warn individuals about potentially infectious contacts can be reached by respective add-ons. Also, the solution is limited in terms of efficiency and hardware requirements.

Apart from this, and as to be expected, the integrability and interoperability of the other architectures decrease with the complexity of supported features, cf. Section 3.1 and Section 3.2.

Regarding supported health checks, it is easy to see that physical checks that do not require identifying information (temperature, mask, etc.) are supported by all architectures. In case of digital checks, which are tied to the identity of the individual, there is an important fact to stress: since in the parallel architecture the coupling of the classical AC and the RiBAC extensions is non-existent, digital checks are not supported in an automated way and would require manual intervention (e.g., checks of ID documents).

4.1 Open Challenges

In order to achieve real preparedness for a potential future health emergency situation, a variety of steps should be taken. On the deployment side, existing AC systems need to be analyzed and the required interfaces, e.g., for the sequential architecture, need to be defined and standardized in order to guarantee compatibility with external infrastructure such as the EUDCC. Furthermore, efficiency benchmarks for the different approaches and on different hardware profiles need to be established, to allow for an easy selection of the appropriate solution for a given setting.

All architectures presented above assume that there is no ambiguity about the user requesting access, which requires, e.g., turnstiles, to avoid tailgating attacks, or to avoid that the temperature of the wrong individual is scanned. While the required infrastructure will typically already exist for traditional AC systems, it is an open challenge especially for the last construction to allow for seamless access control without requiring expensive hardware while still protecting the privacy of individuals in the best way possible.

Especially due to the use of biometrics in Sections 3.2 and 3.3, also the perceived privacy impact and social acceptance play an important role. By raising awareness of existing solutions and educating society, reluctance of adoption (similar to, e.g., digital contact tracing apps) should be pro-actively addressed.

Finally, on the more technical side, additional research regarding privacy-preserving matching of biometrics needs to be carried out in order to improve existing trade-offs with regards to supported biometric features, efficiency, and accuracy.

ACKNOWLEDGMENTS



Co-funded by
the European Union

This work was funded by the European Union through the Horizon Europe research programme under grant agreement n°101073821 (SUNRISE). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

The authors would like to thank Stefan More for detailed and highly valuable comments on a previous version of this document. We are grateful to the anonymous reviewers for their helpful comments and suggestions.

The figures in this document have been designed using images from  flaticon.

REFERENCES

- [1] Carlisle Adams. 2011. Achieving non-transferability in credential systems using hidden biometrics. *Secur. Commun. Networks* 4, 2 (2011), 195–206. <https://doi.org/10.1002/sec.136>
- [2] Carsten Baum, Tore Kasper Frederiksen, Julia Hesse, Anja Lehmann, and Avishay Yanai. 2020. PESTO: Proactively Secure Distributed Single Sign-On, or How to Trust a Hacked Server. In *IEEE European Symposium on Security and Privacy, EuroS&P 2020, Genoa, Italy, September 7-11, 2020*. IEEE, 587–606. <https://doi.org/10.1109/EuroSP48549.2020.00044>
- [3] Jan Camenisch and Anna Lysyanskaya. 2001. An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. In *Advances in Cryptology - EUROCRYPT 2001, International Conference on the Theory and Application of Cryptographic Techniques, Innsbruck, Austria, May 6-10, 2001, Proceeding (Lecture Notes in Computer Science, Vol. 2045)*, Birgit Pfitzmann (Ed.). Springer, 93–118. https://doi.org/10.1007/3-540-44987-6_7
- [4] Jan Camenisch and Anna Lysyanskaya. 2002. A Signature Scheme with Efficient Protocols. In *Security in Communication Networks, Third International Conference, SCN 2002, Amalfi, Italy, September 11-13, 2002. Revised Papers (Lecture Notes in Computer Science, Vol. 2576)*, Stelvio Cimato, Clemente Galdi, and Giuseppe Persiano (Eds.). Springer, 268–289. https://doi.org/10.1007/3-540-36413-7_20
- [5] David Chaum. 1981. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. *Commun. ACM* 24, 2 (1981), 84–88. <https://doi.org/10.1145/358549.358563>
- [6] David Chaum. 1982. Blind Signatures for Untraceable Payments. In *Advances in Cryptology: Proceedings of CRYPTO '82, Santa Barbara, California, USA, August 23-25, 1982*, David Chaum, Ronald L. Rivest, and Alan T. Sherman (Eds.). Plenum Press, New York, 199–203. https://doi.org/10.1007/978-1-4757-0602-4_18
- [7] David Chaum. 1985. Security Without Identification: Transaction Systems to Make Big Brother Obsolete. *Commun. ACM* 28, 10 (1985), 1030–1044. <https://doi.org/10.1145/4372.4373>
- [8] Pau-Chen Cheng, Pankaj Rohatgi, Claudia Keser, Paul A. Karger, Grant M. Wagner, and Angela Schuett Reninger. 2007. Fuzzy Multi-Level Security: An Experiment on Quantified Risk-Adaptive Access Control. In *2007 IEEE Symposium on Security and Privacy (S&P 2007), 20-23 May 2007, Oakland, California, USA*. IEEE Computer Society, 222–230. <https://doi.org/10.1109/SP.2007.21>
- [9] Spela Cucko and Muhamed Turkanovic. 2021. Decentralized and Self-Sovereign Identity: Systematic Mapping Study. *IEEE Access* 9 (2021), 139009–139027. <https://doi.org/10.1109/ACCESS.2021.3117588>
- [10] Amos Fiat and Adi Shamir. 1986. How to Prove Yourself: Practical Solutions to Identification and Signature Problems. In *Advances in Cryptology - CRYPTO '86, Santa Barbara, California, USA, 1986, Proceedings (Lecture Notes in Computer Science, Vol. 263)*, Andrew M. Odlyzko (Ed.). Springer, 186–194. https://doi.org/10.1007/3-540-47721-7_12
- [11] Tore Kasper Frederiksen. 2021. A Holistic Approach to Enhanced Security and Privacy in Digital Health Passports. In *ARES 2021: The 16th International Conference on Availability, Reliability and Security, Vienna, Austria, August 17-20, 2021*, Delphine Reinhardt and Tilo Müller (Eds.). ACM, 133:1–133:10. <https://doi.org/10.1145/3465481.3469212>
- [12] Jesús García-Rodríguez, Stephan Krenn, and Daniel Slamanig. 2023. To Pass or Not to Pass: Privacy-Preserving Physical Access Control. *Cryptology ePrint Archive, Paper 2023/934*. <https://eprint.iacr.org/2023/934>
- [13] Tom Godden, Ruben de Smet, Christophe Debryne, Thibaut Vandervelden, Kris Steenhaut, and An Braeken. 2022. Circuitree: A Datalog Reasoner in Zero-Knowledge. *IEEE Access* 10 (2022), 21384–21396. <https://doi.org/10.1109/ACCESS.2022.3153366>
- [14] Google LLC and Apple Inc. 2020. Google Apple Exposure Notification (GAEN) Framework. <https://www.google.com/covid19/exposurenotifications/> and <https://www.apple.com/covid19/contacttracing/>.
- [15] Jens Groth. 2016. On the Size of Pairing-Based Non-interactive Arguments. In *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part II (Lecture Notes in Computer Science, Vol. 9666)*, Marc Fischlin and Jean-Sébastien Coron (Eds.). Springer, 305–326. https://doi.org/10.1007/978-3-662-49896-5_11
- [16] Julia Hesse, Nitin Singh, and Alessandro Sorniotti. 2023. How to Bind Anonymous Credentials to Humans. *Cryptology ePrint Archive, Paper 2023/853*. <https://eprint.iacr.org/2023/853>

- [17] Chris Hicks, David Butler, Carsten Maple, and Jon Crowcroft. 2020. Secure-ABC: Secure AntiBody Certificates for COVID-19. *CoRR* abs/2005.11833 (2020). arXiv:2005.11833 <https://arxiv.org/abs/2005.11833>
- [18] Emmie Hine, Jessica Morley, Mariarosaria Taddeo, and Luciano Floridi. 2021. Saving Human Lives and Rights: Recommendations for Protecting Human Rights when Adopting COVID-19 Vaccine Passports. *Social Science Research Network (SSRN)* (2021).
- [19] PEPP-PT. 2020. PEPP-PT: High-Level Overview. <https://github.com/pepp-pt/pepp-pt-documentation/blob/master/PEPP-PT-high-level-overview.pdf>.
- [20] Kai Rannenberg, Jan Camenisch, and Ahmad Sabouri (Eds.). 2015. *Attribute-based Credentials for Trust: Identity in the Information Society*. Springer. <https://doi.org/10.1007/978-3-319-14439-9>
- [21] ROBERT. 2020. ROBERT: ROBust and privacy-presERving proximity Tracing. <https://github.com/ROBERT-proximity-tracing/documents/blob/master/ROBERT-summary-EN.pdf>.
- [22] Michael Rosenberg, Jacob White, Christina Garman, and Ian Miers. 2022. zk-creds: Flexible Anonymous Credentials from zkSNARKs and Existing Identity Infrastructure. *Cryptology ePrint Archive, Paper 2022/878*. <https://eprint.iacr.org/2022/878>
- [23] Claus-Peter Schnorr. 1989. Efficient Identification and Signatures for Smart Cards. In *Advances in Cryptology - CRYPTO '89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings (Lecture Notes in Computer Science, Vol. 435)*, Gilles Brassard (Ed.). Springer, 239–252. https://doi.org/10.1007/0-387-34805-0_22
- [24] Abhishek Sharma, Chandana Hewege, and Chamila Perera. 2022. Exploration of Privacy, Ethical and Regulatory Concerns Related to COVID-19 Vaccine Passport Implementation. In *HCI for Cybersecurity, Privacy and Trust - 4th International Conference, HCI-CPT 2022, Held as Part of the 24th HCI International Conference, HCII 2022, Virtual Event, June 26 - July 1, 2022, Proceedings (Lecture Notes in Computer Science, Vol. 13333)*, Abbas Moallem (Ed.). Springer, 480–491. https://doi.org/10.1007/978-3-031-05563-8_30
- [25] TCN Coalition. 2020. TCN Protocol. <https://github.com/TCNCoalition/TCN>.
- [26] Carmela Troncoso, Dan Bogdanov, Edouard Bugnion, Sylvain Chatel, Cas Cremers, Seda F. Gürses, Jean-Pierre Hubaux, Dennis Jackson, James R. Larus, Wouter Lueks, Rui Oliveira, Mathias Payer, Bart Preneel, Apostolos Pyrgelis, Marcel Salathé, Theresa Stadler, and Michael Veale. 2022. Deploying decentralized, privacy-preserving proximity tracing. *Commun. ACM* 65, 9 (2022), 48–57. <https://doi.org/10.1145/3524107>
- [27] Carmela Troncoso, Mathias Payer, Jean-Pierre Hubaux, Marcel Salathé, James R. Larus, Wouter Lueks, Theresa Stadler, Apostolos Pyrgelis, Daniele Antonioli, Ludovic Barman, Sylvain Chatel, Kenneth G. Paterson, Srdjan Capkun, David A. Basin, Jan Beutel, Dennis Jackson, Marc Roeschlin, Patrick Leu, Bart Preneel, Nigel P. Smart, Aysajan Abidin, Seda Gürses, Michael Veale, Cas Cremers, Michael Backes, Nils Ole Tippenhauer, Reuben Binns, Ciro Cattuto, Alain Barrat, Dario Fiore, Manuel Barbosa, Rui Oliveira, and José Pereira. 2020. Decentralized Privacy-Preserving Proximity Tracing. *IEEE Data Eng. Bull.* 43, 2 (2020), 36–66. <http://sites.computer.org/debull/A20june/p36.pdf>
- [28] Binhua Wang and Yuan Ping. 2022. A comparative analysis of COVID-19 vaccination certificates in 12 countries/regions around the world: Rationalising health policies for international travel and domestic social activities during the pandemic. *Health policy* 126, 8 (2022), 755–762.