Designing and Developing a Digital Competency Profile

D. Viliavin[1][a], N. Komleva[2][b], N. Mamedova[2][c] and A. Urintsov[2][d]
[1]*Skolopendra LLC, Kosmodamianskaya embankment, Moscow, Russia*
[2]*Basic Department of Digital Economy, Plekhanov Russian University of Economics, Stremyanny Lane,* Moscow, Russia
mamedova.na@rea.ru

Keywords: Software development, Digital profile, Digital agent, Decentralized application, Identity management, Personal learning trajectory, Self-sovereign identity, Verifiable credentials.

Abstract: The article contains the results of selecting and justifying solutions for designing and developing a decentralized application - a digital competence profile - which is not only a repository of personal data, learning outcomes, digital footprint, but also gives the data holder the opportunity to fully manage them. Emphasis is placed on the possibilities of applying decentralized technologies in development, the SSI approach for effective identity management and the VC credentials storage standard. The proposed solutions are focused on ensuring that the functionality of a digital agent can be fully implemented in a digital competency profile. It is shown how true data portability will be ensured and data protection rules will be observed. Priority functional requirements that should form the basis of the designed decentralized application are given, and software development tools are identified. The results of the study can be applied by software developers in the field of online learning and organization of the Learning Record Store.

1 INTRODUCTION

New development models for modern applications based on decentralization, which include cryptographic transaction logging, peer-to-peer technologies, and a resource-constrained model, are being actively created and formed. Most of the intelligent online learning support applications offered today are centralized - the servers and data of such applications are owned by a specific owner. The centralized approach to the distribution and operation of an application deprives the procedure of working with it of transparency for all participants in the educational process. In addition, the centralized type of digital footprint data storage extremely restricts the process of personalization of learning as well, since the receipt, use and processing of such data, including for the purpose of extracting useful information, is limited to the owner of the application.

Thus, the growth of centralized applications, which was a natural response to the increasing popularity of distance learning in the world [1], has shown the need for the holder of learning data to be the user himself. Modern decentralization technologies have become the basis for providing this need, contributing to the active development of decentralized application development model.

In this regard, the task of designing and developing a digital competency profile, which would accumulate data about a person's learning throughout his life, is relevant. In this case, any actions of the learner during the educational process will be recorded, validated and integrated into the digital competence profile. Tools for collecting and processing the learner's digital footprint (metadata on any forms of activity, on the nature of his interaction with the educational service functions) are used to confirm the acquired competencies.

As you know, the task of software design can be solved in different ways, but first it is necessary to identify and justify the use of a certain stack of technologies and approaches that will ensure the effectiveness, competitiveness and scalability of the development product. This study presents the results of the work performed to prepare a solution for

[a] https://orcid.org/0009-0008-5995-3881
[b] https://orcid.org/0000-0003-0724-1221
[c] https://orcid.org/0000-0002-8934-7363
[d] https://orcid.org/0000-0003-0273-5134

designing a digital competency profile in the form of verifiable credentials in accordance with the Verifiable Credentials (VC) standard [2] and with the further possibility of personalizing the learning process on the platform "Digital Tutor" developed at Plekhanov Russian University of Economics and designed to create personalized adaptive online courses [3].

2 SURVEY METHODOLOGY

The Self-sovereign identity (SSI) approach and the Verifiable Credentials (VC) credential storage standard for validating a learning document have been proposed as the architectural basis for designing a digital competency profile.

The SSI approach provides a digital repository designed to store verifiable credentials and defines the logic for managing them [4]. Comparing a digital profile to a physical wallet, we can use the analogy that a person - a wallet owner - puts credentials into a wallet and takes them out to prove his identity as the owner. The wallet itself cannot perform any activity. With a digital profile, the owner needs software to manage the interactions. This software module is known as the digital agent. Through the digital agent module, the controller, acting on behalf of and with the user's permission, performs all functions as part of the interaction management.

The entities "digital profile" and "digital agent", in terms of the SSI approach, correlate as browsers and servers with the Internet, that is, they are the basic tools necessary for the operation of the entire network decentralized infrastructure. While browsers exchange web pages, the digital profile and the digital agent exchange verifiable credentials (VC).

Despite the seeming simplicity of formulating a digital profile task, the actual workload is quite large. Requirements for security, privacy, cryptography, functionality, portability and usability must be considered. Creating a fully functional SSI profile is the work of designing and developing digital identity software [5].

Current implementations of a digital profile based on the SSI approach include:

- Decentralized identifiers (DIDs - peer-to-peer DIDs, contextual DIDs, publicly available DIDs);
- Verifiable Credentials (VC) owned by the user;
- Digital copies (e.g., PDF files) of physical credentials such as passport, driver's license, birth certificate, diploma, other credentials that have not yet been converted to verifiable credentials;
- Personal data of all categories;
- Formalized or templated personal data (resume, biographical information).

This list does not include data related to cryptocurrencies, digital tokens, and other forms of value exchange. At present, separate profiles are created for them, but in the future such data will become part of digital profiles [6]. As an example, NFT (non-fungible token) technology, widely used in e-commerce, captures the ownership of a digital object by a unique user and allows identifying the owner of a digital or tangible asset. NFTs used to be a separate story and were stored in special wallets. Now, however, they are integrated into a single wallet via plugins or by default.

Figure 1 shows a typical digital profile and digital agent architecture based on the SSI approach.

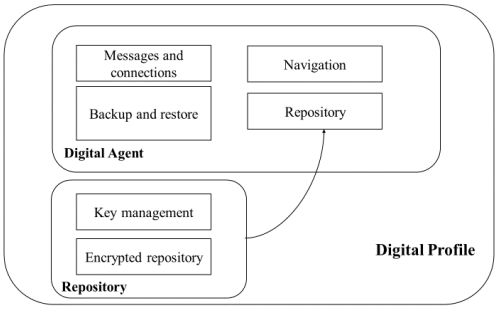

Figure 1: Conceptual architecture of a typical digital profile and digital agent.

A standard for digital profiles, including for transmitting credentials on the Internet in a way that is cryptographically secure, privacy-aware and machine-verifiable, is currently under active development. A draft of such work appeared in August 2020 thanks to the W3C Credentials Community Group team. The draft currently has version 2.0 status and continues to be modified. A list of current W3C publications and the latest revision of this technical report can be found in the W3C Technical Reports Index. This both gives both leeway and imposes restrictions on interoperability between digital agents.

In addition to the ongoing work on the standard, the community is developing and testing experimental specifications that are not suitable for production deployment, but are gradually shaping the documentation area for a single standard. Such specifications include, for example, one that describes mechanisms for ensuring the authenticity and integrity of structured digital documents using

cryptography, such as digital signatures and other digital mathematical proofs, presented by the W3C team.

The SSI approach ecosystem for implementing software solutions in education is represented by several categories of participants: Issuer, Verifier, Holder. The projected digital competence profile, which is a decentralized application, allows the Holder to perform at its own discretion a variety of actions in relation to the data storage (a direct analogy of which is an electronic wallet), in particular to generate, store, manage and protect cryptographic keys, secrets (link secrets), confidential personal data. It should be pointed out that the category "sensitive personal data" includes all kinds of such data. However, all these actions are possible only if the verifiable credentials are accumulated in the digital competence profile.

The Verifiable Credentials (VC) architecture's mechanism for supporting the security and confidentiality of the data being sent is implemented as follows:

- Issuers (organizations and individuals) are the source of verifiable credentials (VC);
- Holders (users) request verifiable credentials from issuers, store them in their digital repository, and provide VC evidence when requested by the Verifier;
- Verifiers (any individual or organization) request evidence from Holders of one or more verifiable VC. If the Holder agrees to the data transfer, the Holder's digital agent returns the proof, which the Verifier can then verify.

An important step in this process is the verification of the Issuer's digital signature, typically performed using a Decentralized Identifier (DID). The Verifiable Data Registry (VDR) is the place to which the decentralized identifier is attached. Each participant communicates with each other using a DID.

Thus, in the VC architecture, the Holder makes its own decisions about the management of verifiable credentials. The Issuer sends the identity attributes to the Holder as VC content, then the Holder decides what to do with them next, similar to the user's actions with confirming physical documents.

The trust model in the identity management system in the VC architecture is shown in Figure 2. It shows the relationship of the three main participants - Issuer, Holder and Verifier - with three technical components: the Holder's digital agent, the Holder's vault and the blockchain-based verifiable data registry (VDR).

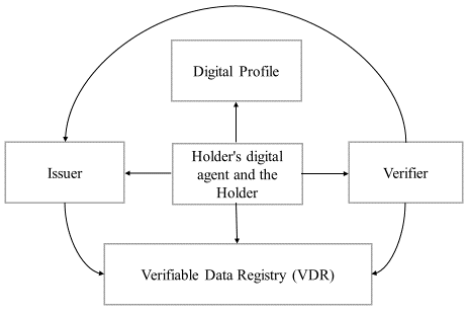

Figure 2: Trust model in identity management system in Verifiable Credentials architecture.

The trust model presented is essentially the same as the trust model in place for physical documents [7]. This is one of the main strengths of the Verifiable Credentials architecture for the simple reason that it works the same way as trust in the real world - there is no third party in the form of the Issuer who determines all Holder interactions.

Selective disclosure is another convenient privacy feature that the VC architecture supports. Figure 3 shows an example of disclosed credentials containing information about the Holder's education level.


```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://schema.org"
  ],
  "id": "http://example.edu/credentials/1234",
  "type": [
    "VerifiableCredential",
    "Course"
  ],
  "credentialSubject": {
    "id": "did:example:bca123456",
    "educationalCredentialAwarded": "Бакалавр направления подготовки
      Математическое обеспечение и администрирование информационных
      систем"
  },
  "issuer": "did:example:abcdef123456",
  "issuanceDate": "2021-05-15T13:25:51Z",
  "expirationDate": "2019-05-15T14:04:07Z"
}
```


Figure 3: Example of selective VC disclosure.

There are two main ways of selective disclosure:

- By including only an absolute minimum number of properties (preferably one) in a single VC (so-called atomic VC);
- By using VC with proof of zero disclosure (ZKR).

In the first case, instead of issuing a complex VC containing several properties, the Issuer issues a set of atomic VCs. For example, a complete online course VC contains a significant amount of recorded information, whereas it can be divided into a set of atomic VCs, each containing a single action and an ID link to link all the VCs together. The Holder can then selectively disclose individual properties of the

course completion, whether it is the results of the final activities or the certificate of completion received.

The atomic VC logic can follow the xAPI educational standard and provides the retention of learner activity information required by the standard. At the same time, the level of detail in recording this information can be different.

Zero-disclosure proofs are used to validate information regarding an individual's credentials without having to fully disclose other sensitive personal information. Every scenario in which one needs to prove that an individual is entitled to access a service without disclosing more personal information than necessary is a potential application for ZKP [8].

To develop a personal learning trajectory, in particular, the module "Personal Trajectory" in the project "Digital Tutor" adopted the option of obtaining full digital footprint data, which contains information about the activity of the learner. This option implies the choice in favor of the second method of selective disclosure of information - by using VC with proof of zero disclosure.

3 RESEARCH RESULTS

The new generation of digital profiles and digital agents developed using the SSI approach is not like the previous one - the design principles have changed. Following the changes, the design of a digital competence profile must be done outside the proprietary limitations of APIs controlled by individual software vendor developers, since such limitations prevent the transfer of credentials to the digital competence profile.

According to the first principle, when developing a digital competency profile based on the SSI approach, open standards for DIDs, cryptographic keys, verifiable credentials (VC), and any other user-controlled storage content must be implemented. This allows the controller through the digital agent to have true data portability, that is, the ability to move the contents of its digital profile to another vendor profile or between its profiles at any time.

This implies that multiple digital profiles and digital agents from different vendors must be able to interact on behalf of the same controller, whether it is a person with multiple devices (e.g., smartphone, tablet, laptop) or an organization with different operating systems and applications from different vendors (not to mention employees using a variety of devices and operating systems).

At the moment, the level of digital trust is not high enough to fully implement the first principle when designing a digital competency profile. The fairly common requirement to use only certified and accredited devices limits portability, but there is reason to increase the level of digital trust, and the prospects are very optimistic [9].

The second basic principle of digital competency profile design is the confidentiality of the nature and value of digital profile content. This principle can be implemented through observance of the condition that a digital agent never takes actions not authorized by its controller.

This does not mean that a digital agent interacts with a controller every time a data transaction is performed, for the sake of obtaining consent. Agents can be designed to remember the policies and preferences of their controllers and automatically perform certain actions with controller sanction. A common example, already widely implemented in banking, is automatic payment of recurring bills. The account owner sets the rules, and the bank's internal systems will automatically pay certain bills.

Implementing the second principle when designing a digital competency profile enables compliance with data protection rules, in particular the requirements of the General Data Protection Regulation (GDPR). And at the same time, it allows users to track when and where they shared sensitive personal data and manage it qualitatively - to track the distribution, update or delete it.

The projected digital competency profile is focused on ensuring that digital agent functionality can be fully implemented. This includes, but is not limited to:

- Messaging. A digital agent functions roughly like a specialized email or chat application - it knows how to send and receive data, structure messages, and push notifications on behalf of the controller;
- Routing. A digital agent that represents an organization serves as an intermediary for routing other messages from agent to agent using protocols, such as DIDComm, designed to organize multi-agent routing. DIDComm emerged from the Hyperledger Aries project and was standardized by the DIDComm working group at the Decentralized Identity Foundation;
- Backup and Recovery. Given the value and sensitivity of the data stored in a digital competency profile, it is important that it supports robust backup and recovery capabilities in the event of loss, corruption, or

hacking of digital profile software and/or hardware and digital agent;

- Secure Storage. One of the important components of a digital agent that interacts with digital profile services. For example, through the API provided by the digital profile.

The implementation of these principles in the design of the digital competency profile also determines its structure, which includes, in particular, two main components:

- Key Management System. The main functions of the digital competence profile: processing the creation, revocation, storage, signing and protection of cryptographic keys and related secrets, such as reference secrets used in zero-disclosure evidence;
- Encrypted Storage. The second main function of the profile is the secure storage of keys, secrets and other personal data that the controller chooses to store in it.

3 DISCUSSION OF RESULTS

The digital competency profile should be designed to meet the following priority functional requirements:

- Security of storage data;
- Ease of use on a variety of devices;
- Accessibility to expansion and integration with the Learning Record Store (LRS) subsystem, which contains information about learning activities, forming a digital trail and recording in databases the actions performed by the learner.

Software tools designed on the basis of a distributed registry should be able to quickly process queries within the network with minimal load on the device. The use of the programming language Rust and the frameworks Hyperledger Aries and Indy was recommended to develop the digital competency profile. The programming language was chosen because of the need for safe programming and an accurate understanding of how a particular piece of code works. With support for the main programming paradigms: object-oriented, parallel, functional and procedural, Rust is universal and easy to write software. With the help of this language and develop the selected frameworks, which will allow to implement the creation, storage, exchange and validation of obtained Verifiable Credentials.

The solution is based on the results of the analysis of a number of positive practices in the implementation of projects in the studied subject area: Exonum (a framework for the creation of blockchain projects), MaidSafe (distributed system of data storage and processing), Solana (platform for creating blockchain applications), Hyperledger Indy and Aries (frameworks to implement blockchain and SSI technology). Work in this area is ongoing and other solutions are possible. The security of the storage data is proposed through the use of blockchain technology and cryptographic methods [10]. This will allow verification of the stored information with a zero-disclosure proof.

4 CONCLUSIONS

The relevance of the designed software tool - digital competence profile - is due to the need of a person to manage his achievements accumulated in the learning process. The efficiency of the implementation of the digital competence profile is calculated on the specific procedures of the educational process and consists in a multiple reduction of cost and labor costs due to the automation of data authentication process. It is important to note that the software tool being designed can be applied in solving any tasks in which an individual is required to confirm the competencies he/she has acquired.

REFERENCES

Imed Bouchrika, *50 Online Education Statistics: 2023 Data on Higher Learning & Corporate Training*, URL: https://research.com/education/online-education-statistics.

Verifiable Credentials Data Model v1.1, *W3C Recommendation*, 03 March 2022 URL: https://www.w3.org/TR/vc-data-model.

Komleva, N., Vilyavin, D., 2020. Digital platform for creating personalized adaptive online courses. *Open education*, 24(2):65-72.

Mühle, A., Grüner, A., Gayvoronskaya, T. and Meinel, C., 2018. A survey on essential components of a self-sovereign identity. *Computer Science Review*, 30:80–86.

Solenyi, S., Voropaev, S., 2022. On the introduction of verifiable credentials (VC) and decentralized identifiers (did) into the authentication system, *Zavalishinsky readings 22 : Collection of reports of the XVII International Conference on Electromechanics and Robotics, St. Petersburg*, April 12-14, 2022. – Saint Petersburg: Saint Petersburg State University of Aerospace Instrumentation. pages 58-61.

Ante, L., 2022.The Non-Fungible Token (NFT) Market and Its Relationship with Bitcoin and Ethereum. *FinTech*. 1(3):216-224.

Zero Trust Architecture. *National Institute of Standards and Technology Special Publication*, 800-207, 59 p. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

Konkin, A., Zapechnikov,S., 2021. Privacy methods and zero-knowledge poof for corporate blockchain, *Procedia Computer Science*,Volume 190. pp. 471-478.

Digital Trust Survey Report 2022 // DigiCert URL: https://www.digicert.com/content/dam/digicert/pdfs/report/state-of-digital-trust-survey-report-en.pdf.

Liu, Y., He, D., Obaidat, M., Kumar, N., Khurram Khan, M., Choo, K-K R., 2020. Blockchain-based identity management systems: A review. *Journal of network and computer applications*, 166:102731.