BLOCKCHAIN™ IN HEALTHCARE TODAY

ORIGINAL CLINICAL RESEARCH

Evaluation of Decentralized Verifiable Credentials to Authenticate Authorized Trading Partners and Verify Drug Provenance

Ghada L. Ashkar, PharmD[1], Kalpan S. Patel, PharmD, MBA[1], Josenor de Jesus, PharmD, MBA, FACHE[1], Nikkhil Vinnakota[2], Natalie Helms[2], Will Jack[3], William Chien, PharmD, MBA[3] and Ben Taylor[3]*

[1]UCLA Health, Los Angeles, CA, USA; [2]Amgen, Thousand Oaks, CA, USA; [3]LedgerDomain, Las Vegas, NV, USA

Abstract

***Summary*:** In 2013, the Drug Supply Chain Security Act (DSCSA) was signed into law to address the growing threat of counterfeit drugs and to ensure prescription drugs remain safe and effective for patients. As part of this law, US pharmaceutical supply chain stakeholders are required to confirm the authorized status of trading partners for transactions and information disclosures, even when there is no prior business relationship. While larger Authorized Trading Partners (ATPs) have connectivity solutions in place, newer and smaller ATPs have not traditionally participated, including tens of thousands of dispensers. To unlock the full potential of the interoperable system mandated by the DSCSA, the authors tested eXtended ATP (XATP), a blockchain-backed framework for ATP authentication and enhanced verification in a real-world pharmacy with genuine drug packages. The objective of this research study was to prove that electronic authentication and enhanced verification can be achieved between ATPs using a mobile-based solution. Moreover, we tested accurate reading of drug and associated electronic med guides, flagging of expired and recalled drugs, and correct generation of documentation to support saleable returns.

***Methods*:** This study involved two dispensers and three participating manufacturers. Dispensers were onboarded to a mobile application and used supporting documentation to authenticate their identities, and then scanned 2D drug barcodes to submit drug verification requests to manufacturers (including 11 additional, randomly selected manufacturers). Genuine and synthetic drug package barcodes were used to test workflows against genuine and synthetic manufacturer serialization data records. Manufacturers authenticated the identity of requesting dispensers with verifiable credentials and responded to verification requests.

***Results*:** Enhanced drug verification was achieved, with 100% of requests successfully delivered to participating manufacturers and 88% of requests being delivered to other manufacturers (based on the pharmacist selection of random packages from the pharmacy). Drug verification matching against synthetic serialization data records resulted in 86% accuracy, with the 14% error rate attributed to human factors. All barcodes were successfully scanned and provided package-accurate data, and 97% of randomly selected packages successfully generated drug package inserts. All synthetic recalls and expired drugs were successfully flagged. Four of the manufacturers contacted were among the top 15 pharmaceutical manufacturers globally; all four responded.

***Conclusions*:** The XATP framework provides a secure, reliable, and seamless remote method to conduct enhanced verification as required by law. Interoperability between manufacturers and dispensers with no prior business relationship can be achieved on 'day zero' using mobile devices that enable digital authentication and rapid barcode scanning. As users retain control of their own private keys, the framework also mitigates the single-point-of-attack risks associated with centrally managed systems.

Keywords: *verifiable credentials; identity; DSCSA; pharmaceutical supply chain; drug verification*

Received: 9 February 2021; Revised: 17 February 2021; Accepted: 17 February 2021; Published: 11 March 2021

Over the past two decades, globalization and technological innovation have profoundly changed the US pharmaceutical supply chain, and thus, stakeholders face new and emerging requirements under the Drug Supply Chain Security Act (DSCSA) (1). One such requirement is an example of a 'know your customer'

*Correspondence: Ben Taylor. Email: ben.taylor@ledgerdomain.com

(KYC) requirement (2), in which each Authorized Trading Partner (ATP) (3) is required to confirm that their trading partner is also authorized (4).

As a result, tens of thousands of ATPs are responsible for authenticating each other's identities before they can transact with one another, or even share certain information – even when there is no prior direct business relationship. While Verification Router Services (VRS) (5) have served to handle drug verifications for saleable returns as required under DSCSA (6), trading partner identity and status authentication remain a missing piece of the puzzle, especially for the broader community of small trading partners (7).

To address this challenge, the authors workshopped and tested a framework for ATP authentication, verification routing, and saleable returns documentation (8). Previously, a working group with representatives from the manufacturing and dispensing sectors found that this framework was capable of onboarding entities and their representatives, accrediting their licenses, and allowing them to share information with unique verifiable credentials (9). The study outlined in this article took the framework out of the virtual conference room and into a real-world production environment.

Under this framework, a dispenser with an iPhone and acceptable form of ID can be remotely authenticated as an ATP, can scan the 2D barcode from a serialized drug in their hand (10, 11), and can use an iOS app to send a verification request (12). This request, which pulls the drug's GS1 Serialized Global Trade Item Number (SGTIN) (13, 14) from the scan, is used to identify the appropriate point of contact (POC) for the manufacturer or repackager. An email is sent asking the POC for validating each scanned drug against its master serialization record. The response can be used to generate supporting documentation to another ATP for a transaction (such as a saleable return (15)).

Technical specifications

The XATP framework consists of five major components:

1. passwordless frontend mobile phone application (also called XATP),
2. application framework encompassing smart contracts and application logic (DocuSeal),
3. notification and verification service (Oraculous),
4. blockchain application server (Selvedge), and
5. backend blockchain (Hyperledger Fabric).

Users generate and hold their own private keys, and master National Drug Code (NDC) data are held locally on the client. Leveraging prior work with UCLA Health and Biogen (16), the Oraculous Interoperability Service unlocks interoperability between existing relational database management systems and hosted nodes of the distributed ledger (17). In this way, verification requests can be submitted, routed, and processed without the need for verifying organizations to provision their own nodes.

The framework leverages proven third-party services, including Splunk (analytics), Branch (mobile link service), OneSignal (push notifications), and Mailgun (email service). Cloud hosting and processing were achieved with LevelDB, Docker, Amazon EC2, Amazon Web Services, and MinIO. The Selvedge blockchain server was built with Golang on top of open-source Hyperledger Fabric 1.4 (Linux Foundation) components (18). Sealed documentation, private metadata, and Product Verification Certificates were held in private storage using MinIO, and public hash records were kept on the blockchain (8).

Objectives

The earlier work of the XATP Pilot Group was conducted remotely using synthetic data in a closed environment. The objective of this study described in this article was to test the application framework in a real-world setting (the UCLA Specialty Pharmacy) using genuine drug packages and manufacturers' production serialization data records.

Specifically, the objectives of this study were to test the following:

1. accurate reading of drug and associated electronic med guides,
2. expired and recalled drug flagging functionality,
3. authentication of a verification request with a verifiable credential, and
4. enhanced verification between dispensers and manufacturers.

Methods and findings

This study included two rounds of testing with three sets of participants: dispensers, participating manufacturers, and other manufacturers based on packages randomly selected from the pharmacy (Table 1).

Table 1. Overview of study participant groups

Group	Members	Location
Dispensers	Pharmacy workgroup consisting of one pharmacist-in-charge (PIC) and two pharmacists (dubbed 'POAs', as they are designated through Power of Attorney to act on behalf of the PIC for the purposes of day-to-day operations)	UCLA Specialty Pharmacy
Participating manufacturers	Members of three pharmaceutical manufacturer organizations (among the top 15 pharmaceutical manufacturers globally) who participated in Zoom tests	Remote
Randomly selected manufacturers	Members of 11 pharmaceutical manufacturer organizations based on drug packages selected randomly from pharmacy inventory by the pharmacist	Remote

Citation: Blockchain in Healthcare Today 2021, **4**: 168 - http://dx.doi.org/10.30953/bhty.v4.168

Dispensers fulfilled their role using the XATP application and iOS email clients, while manufacturers used platform-agnostic email clients and web interfaces. The dispensers and participating manufacturers used Zoom for real-time communication.

Prior to submitting verification requests, dispensers were onboarded to the XATP application and were required to authenticate their identities with supporting documentation. PIC documentation was routed to an external validator, as shown in Fig. 1. Conversely, POA documentation was sent to the PIC, as only the PIC has the authority to authenticate and confer Power of Attorney (POA) to other pharmacy employees (19). In this way, the PIC and POA form a single pharmacy workgroup.

During the course of testing, dispensers submitted drug verification requests to participating manufacturers, as well as to randomly selected manufacturers, based on drug packages selected randomly from pharmacy inventory by the pharmacist. Manufacturer users were able to respond to verification requests embedded in messages encompassing the verification request and the verifiable credential of the requestor. These messages took the form of emails, which could be independently verified by the responder, as shown in Fig. 2.

Round 1

In the first round of testing, 30 genuine drug packages with barcodes were used to test package and medication guide (20) accuracy, and 39 synthetic barcodes were used in combination with pilot manufacturer emails (sent to non-production email addresses at the manufacturer) to test expiration flagging and routing of verification requests (Table 2).

Prior to the test, participating manufacturers were provided with synthetic serialization data records (collectively totaling 1,008 records), and dispensers were provided with 39 synthetic barcodes. Twenty-three of these barcodes corresponded to records in the databases (and could be 'verified'), while 16 did not (and were notionally 'counterfeit'). It should be noted that no actual counterfeits were uncovered through the course of testing.

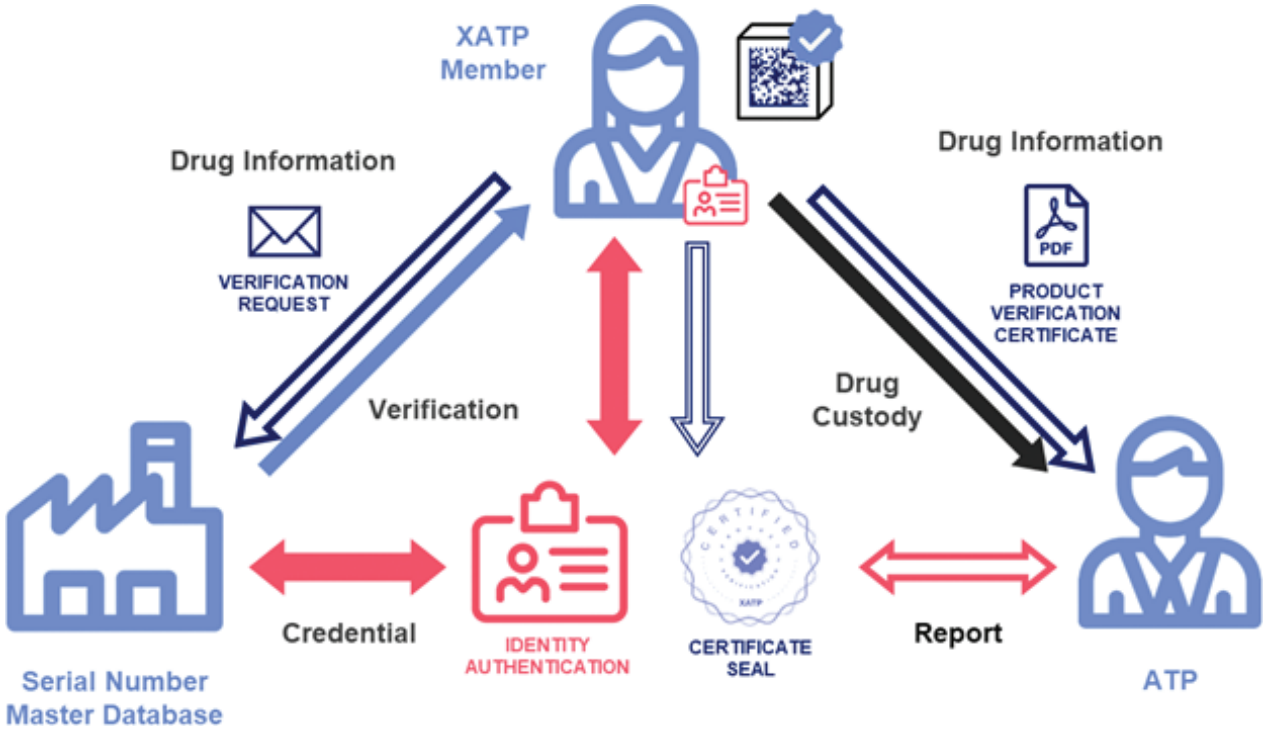

Fig. 1. An overview of the XATP identity framework and enhanced verification routing. After authenticating his or her identity with an independent external validator, the dispenser can scan 2D barcodes on drug packages using an iOS app and submit verification requests as part of the saleable returns process. The package labeler (manufacturer or repackager) receives an email with a verifiable credential and buttons that link to secure Oraculous endpoints, allowing him or her to indicate that a drug is verified or unverified. This verification can be used to generate Product Verification Certificates that can be shared with, and independently authenticated by, other ATPs.

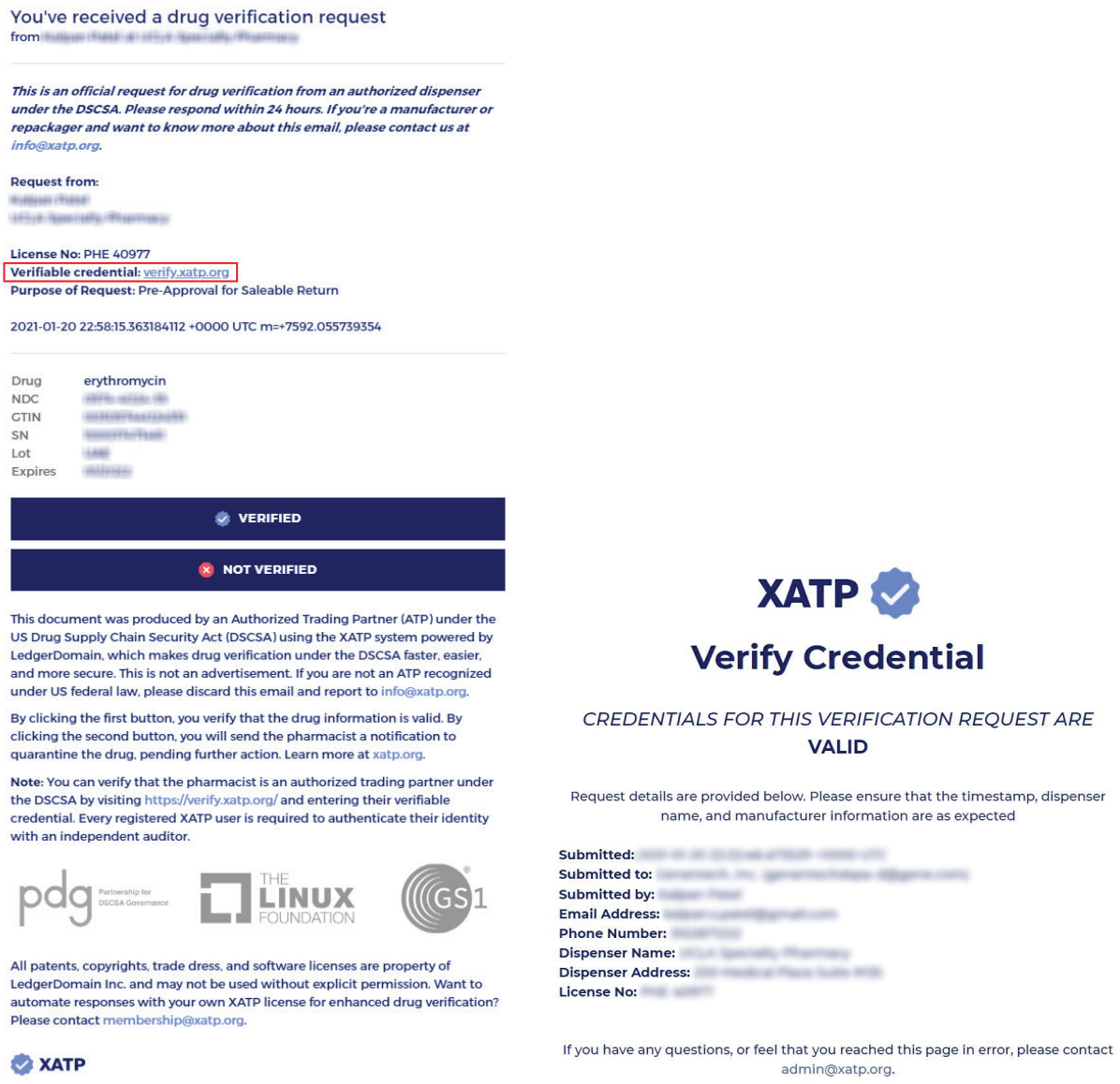

Fig. 2. (Left) An enhanced verification request received by a manufacturer, with a verifiable credential link highlighted in red. (Right) An identity credential verification hosted at a secure web endpoint.

Table 2. Round 1 test objectives, methods, and results

Objective	Data source	Method	Results
Test package and medication guide accuracy	30 genuine drug packages, selected at random from the pharmacy	Three dispensers each scanning 10 packages, confirming package and med guide accuracy	• 100% (30/30) success rate in accurate drug scanning • 97% (29/30) success rate in looking up electronic drug package medication guides
Test routing of synthetic verification requests (dispenser side)	39 synthetic drug packages, consisting of two different manufacturers and six different drugs (including 12 expired drugs)	Two dispensers scanning synthetic drug packages and observing app behavior	• 100% (39/39) success rate in accurate drug scanning • 100% (39/39) success rate in submitting drug verification requests • 100% (39/39) success rate in receiving drug verification status updates • 100% (39/39) success rate in identifying expired drugs
Test routing of synthetic verification requests (manufacturer side)	Emails generated from scanning of 39 drug packages and synthetic serialization data records	Two manufacturers receiving and manually reviewing extracted synthetic barcode data against synthetic serialization data records	• 100% (39/39) success rate in receiving verification requests • 86% (32/39) accuracy in drug verification matching against synthetic serialization data records • 100% (39/39) success rate in responding to verification requests

Citation: Blockchain in Healthcare Today 2021, **4**: 168 - http://dx.doi.org/10.30953/bhty.v4.168

As shown in the table, the authors observed a 100% success rate in submitting, receiving, and responding to drug verification requests on the part of both dispensers and manufacturers. Owing to human factors, 32 of 39 verifications (86%) were successful, as there were four false negatives and three false positives.

Round 2

The second round of testing focused on testing enhanced verification with genuine drugs (Fig. 3), with both participating and randomly selected manufacturers (Table 3).

Table 3. Round 2 test objectives, methods, and results

Objective	Data source	Method	Results
Test routing of genuine verification requests to participating manufacturers	37 genuine drug packages originating from participating manufacturers, selected from the pharmacy	Two dispensers scanning synthetic drug packages and observing app behavior	• 100% (37/37) success rate in accurate drug scanning
	Emails generated from scanning of 37 drug packages and genuine serialization data records	Three manufacturers receiving and manually reviewing extracted genuine barcode data against genuine serialization data records	• 100% (37/37) success rate in receiving verification requests • 100% (37/37) success rate in responding to verification requests
Test recall flagging functionality	Five synthetic drug packages with barcodes corresponding to FDA recalls	One dispenser scanning synthetic drug packages	• 100% (5/5) success rate in identifying the recalled product
Test routing of genuine verification requests to randomly selected manufacturers	27 genuine drug packages selected at random from the pharmacy (resulting in 11 randomly selected manufacturers)	One dispenser scanning genuine drug packages and sending verification requests	• 100% (27/27) success rate in accurate drug scanning • 88% (23/27) success rate in submitting drug verification requests
Test verifiable credential	Two verifiable credentials included in emails to manufacturers	Two manufacturers authenticating emailed requests	• 100% (2/2) verifiable credentials successfully authenticated

During this round, 64 packages were scanned, in total. As three NDCs comprising four products could not be matched to manufacturer POCs, 60 verification requests were submitted and 60 emails were confirmed to have been sent. Overall, the authors observed a 94% success rate in submitting drug verification requests, with the 6% attributed to smaller manufacturers outside the global top 1,000 pharmaceutical companies (21).

Post-round evaluations

Following the completion of Round 2, the authors evaluated the independent verifiability of the drug verification requests, as well as the Product Verification Certificates generated by the pharmacy workgroup. They also received feedback from participating and selected manufacturers.

For the drug verification requests, participating manufacturers tested and successfully authenticated the associated identity credential shown in Fig. 2. This credential, which is linked in the email and is hosted at a secure web endpoint, enables responders to ensure that an email from a requestor is genuine (and not a counterfeiter attempting to gather sensitive information). One of the manufacturers reported that emails had been routed to the incorrect contact. The dispensers and another manufacturer encountered difficulties with the emails, which was found to be the result of link wrapping services executed by their organizations' IT security policies. This required resubmission of verification requests and pointed to the need for domain whitelisting to ensure secure interoperability.

As noted previously, dispensers have the ability to generate Product Verification Certificates that can be shared with, and independently authenticated by, other ATPs. This provides the name, GTIN, NDC, serial number, lot number, expiration date, and verification status for each unit listed. As shown in Fig. 4, each Certificate also bears a URL and access token to a web portal where the user can access its corresponding Certificate Seal, which can be used to authenticate the Certificate. This process can facilitate a verifiable record to show that drugs being received by a third party have been verified and may be sold.

The Certificate Seal includes a list of drugs and their verification statuses, but contains only truncated drug information (22). Certificate holders have the ability to access the Seal and compare it with the data on the Certificate, making it possible to ensure that their Certificate is genuine and untampered. The authors employed Certificate and Seal for analysis of the study results, and found that the former could be successfully authenticated by the latter.

After the round, five of the 14 manufacturers contacted sent verifications in a timely manner: the three participating manufacturers, another global top 15 manufacturer, and a specialty manufacturer. The authors were also contacted by two randomly selected manufacturers requesting additional information regarding the verification requests. One was based outside the United States and directed dispensers to its US subsidiary; the other indicated that requests are preferably routed through a proprietary VRS (a functionality common for wholesale distributors

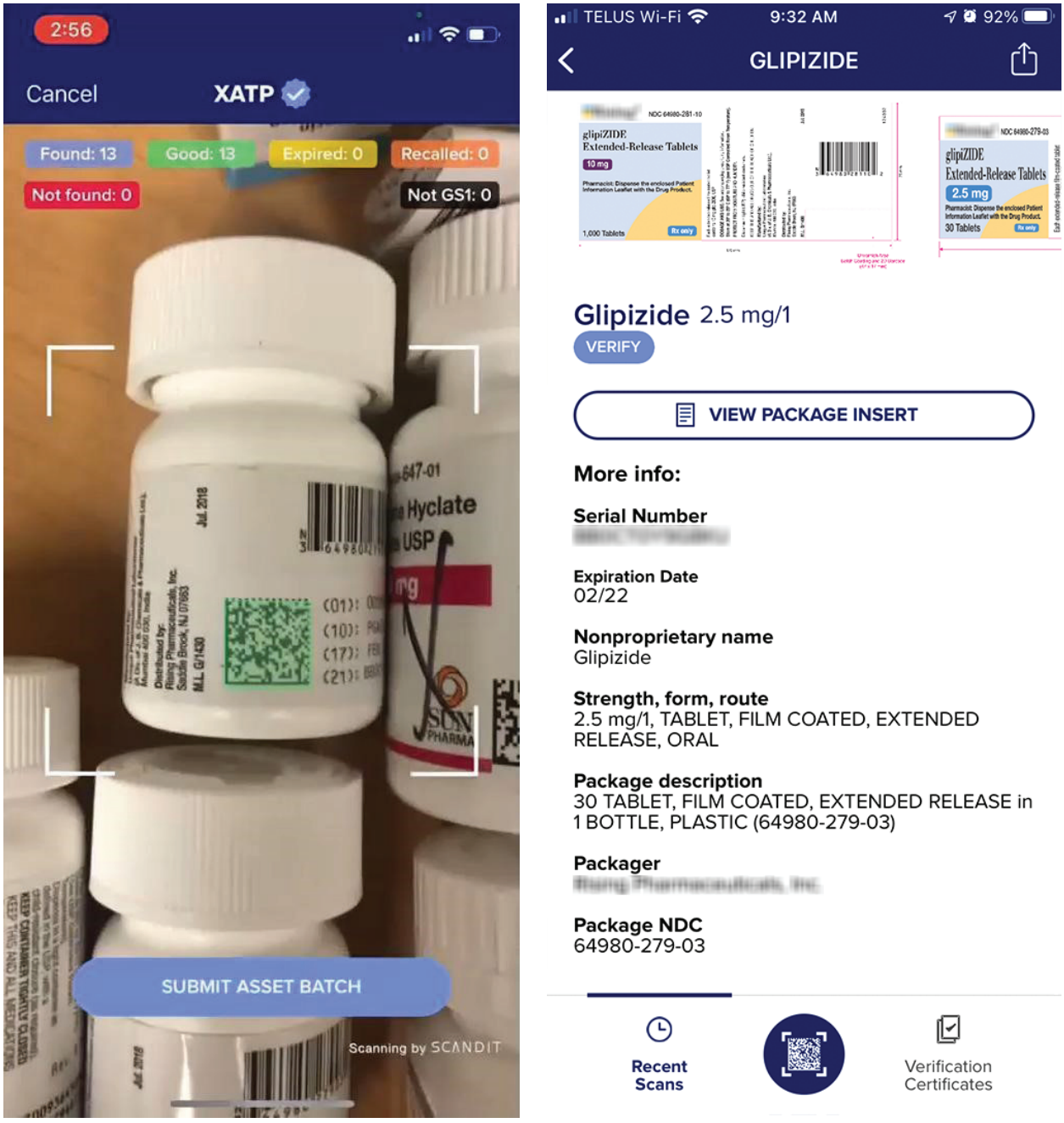

Fig. 3. (Left) Genuine barcodes being scanned at the pharmacy. (Right) The scanned drug in the XATP app.

in verification of saleable returns, but requiring expansion to the broader ATP community).

Discussion and conclusions

In this study, the authors tested a framework for ATP authentication, enhanced verification, and saleable returns documentation in a real-world setting using both genuine and synthetic drug packages to test positive and negative verification workflows. Synthetic recalls and expired drugs were successfully flagged, and 94% of genuine drug verification requests were successfully delivered to participating and randomly selected manufacturers. Each manufacturer was only able to access his or her own verification requests.

Once the identity and ATP status of the PIC were successfully authenticated by an external validator, the PIC, in turn, was able to authenticate POAs, forming a pharmacy workgroup. Within the workgroup, the PIC and POAs shared a common pool of scanned barcodes and Product Verification Certificates, and

Citation: Blockchain in Healthcare Today 2021, **4**: 168 - http://dx.doi.org/10.30953/bhty.v4.168

Drug	NDC	GTIN	SN	Lot	Exp	Status
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Verified
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Not Verified
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Verified
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Verified
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Pending
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Verified
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Verified
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Verified
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Verified
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Verified
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Verified
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Verified
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Verified
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Not Verified
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Verified
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Not Verified
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Not Verified

SN	STATUS
10093114749461	Verified
10023132347438	Not Verified
10000924177801	Verified
H3THVY81R07RAF	Verified
100000198044	Pending
49012433980	Verified
THogUoBjm5gdQCYN	Verified
TL6vZWceK7Yxi7A6	Verified
BCXte7CxVQNNT4bc	Verified
hjBvhzwiVECNPV3P	Verified
xPZnw5WaibXz7ABg	Verified
aAAF8FDZDjVCzexJ	Verified
HDTBAJd6kqJrcFk9	Verified
Wr9uU4qnRGpMPkKC	Not Verified
bYhiCcm5o6ocKEgW	Verified
mZrYNWd3jjvuV6oh	Not Verified
Axx6qDiYY3NkhbAX	Not Verified
qyinhjQCDpY6nW4u	Not Verified
zdED73Ep88sbyGTd	Not Verified
6UCTsVrRWqVQgVf8	Verified
53RYRvbLwstuc4We	Not Verified
JbaoVwnJJxgpAeuL	Not Verified
6RsfXYTqihcYR9RW	Verified
aLv6y4pSVfx7yFzv	Verified
SdVEHjo7LrtrdDqP	Not Verified
KXAmWKN4UACJhMUG	Not Verified
ncvqSGMNJDuw8Jh4	Verified
xxAHJfZigr8qFNxY	Verified
uM3Qc7BFidVwh4iN	Not Verified
NZjQooZgaF6DNhKG	Verified
3DbG8SQn2N7pL3jV	Not Verified
NTPSG6SHcqefryUu	Verified
afRjTGPUzxrbqvpj	Not Verified
4kzB3SmjXEHNvTu3	Verified
cUS5wMMpBpEHh7sP	Not Verified
5tDYDG7heZxPjap5	Verified
rJJREEd5dGg2iLYo	Not Verified
Ge4NN74DYfPmDGkv	Verified
7tyqa7yVFFFNVGEt	Not Verified
Sog7jPUNPXQLhped	Not Verified
LjrCAxdLFA4M42Ja	Not Verified

Fig. 4. (Left) The first page of a Product Verification Certificate generated by a dispenser. (Right) The first page of the corresponding Certificate Seal. Note that in both cases the 'not verified' statuses refer to synthetic barcodes tested during Round 1.

were able to see verification statuses updated in real time. Each dispenser user held his or her own locally encrypted private key, which was generated in concert with signup.

Outside the pharmacy workgroup, other ATPs were proven able to interact with the XATP framework using email clients and web browsers, without the need to install new software or create accounts. Manufacturers received verification requests signed with verifiable credentials, which could be independently authenticated, and were able to respond with the click of a button. Dispensers generated supporting documentation in the form of Product Verification Certificates, which were also independently verifiable.

By directly addressing the need for ATPs under the DSCSA to have a secure, reliable, and seamless remote method for digital IDs, in combination with commercial off-the-shelf mobile phones (23), the framework outlined in this study allowed for 'day zero' interoperability between manufacturers and dispensers with no prior business relationship. All of the major pharmaceutical companies that were contacted sent verifications in a timely manner.

While the study framework involved human-in-the-loop workflows (Fig. 5), the authors anticipate that scaled implementations can be partially or fully automated through existing integration to manufacturer serialization data sources. Once provisioned with agents to test verifiable credentials, machine-to-machine connections between the framework and manufacturer relational databases would manage identity credentials and automatically respond to and sign verification requests. Interoperability with other frameworks could be achieved with an API that enables third parties to make verification requests.

Critically, by ensuring that private keys are held by stakeholders as part of a robust identity system, the XATP framework mitigates the single-point-of-attack risks of legacy providers, where the keys to responder databases are often held and pooled. Much like a janitor's keyring, which grants access to every room in a building, a single security breach in such systems might allow attackers to hijack other identities, create false identities, or gain access to confidential data (24, 25, 26, 27). By allowing for passwordless access closely associated with a device, XATP also sidesteps the risks associated with passwords, including sharing, leaks, and sharing passwords across multiple services (28, 29, 30). The XATP framework thus mitigates the risk for stakeholders to rapidly attain compliance with DSCSA obligations, such as drug verification, and sets a path for greater interoperability leveraging verifiable credentials (31) in the broader healthcare community.

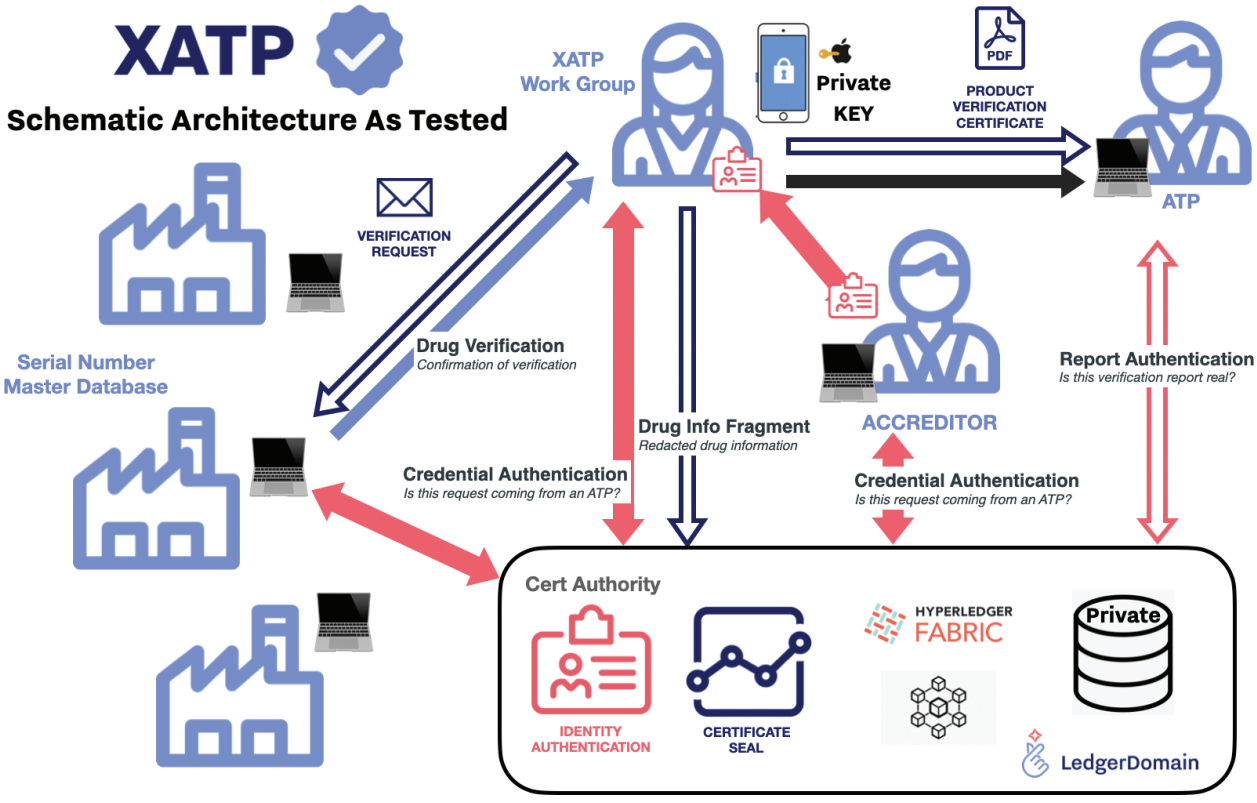

Fig. 5. The framework architecture as tested in this study.

Acknowledgments

The authors thank UCLA Health under the leadership of CEO Johnese Spisso. Special recognition is due to Vidya Rajaram, Mark Karhoff, Nirmal Annamreddy, and Kathy Daniusis (all of Genentech, a member of the Roche Group) and Arthi Nagaraj (of Sanofi) for their contributions to the study effort as participating manufacturers. Their contributions to the journal paper are meant to provide clarification, technical accuracy, and considerations to clearly articulate the learnings from the pilot. Anita Baijnauth of SLADG Notarization served as the independent external validator.

The authors also thank Mike McKinley of UCLA Health, Alina Grigorian of Amgen, Greg Plante of IQVIA, Todd Barrett, RPh of Providence Health, and Ben Nichols of LedgerDomain for their contributions as members of the XATP Working Group. In addition, the authors thank Jose Arrieta (formerly US Department of Health and Human Services); Paul Hackett (Accenture); Diane Shoda (Greyscaling); Alan Lodder, RPh (formerly Intermountain); Dr. Leo Alekseyev, Rick Burgess, Alex Colgan, Dr. Victor Dods, and Mike Lodder (LedgerDomain); Ann Mehra (Splunk); Mike Marchant (UC Davis); and Jennifer Colon, PharmD (Yale).

Conflict of interest and funding

The authors declare no potential conflicts of interest. The study was a joint collaboration of LedgerDomain, UCLA Health, Genentech, Sanofi, and Amgen, and had no external funding.

Authors' contributions

The LedgerDomain team developed the XATP framework in collaboration with the other members of the XATP Working Group. UCLA Health tested the framework with genuine drugs at the specialty pharmacy. Amgen verified drugs as a participating manufacturer. All authors contributed to the conception, development, and writing of this research article.

References

1. U.S. Department of Health and Human Services Food and Drug Administration. Drug Supply Chain Security Act (DSCSA). U.S. Department of Health and Human Services

Food and Drug Administration. Available from: https://www.fda.gov/drugs/drug-supply-chain-integrity/drug-supply-chain-security-act-dscsa [updated 22 May 2019; cited 4 February 2021].
2. Callahan J. Council post: Know Your Customer (KYC) will be a great thing when it works. Forbes; 2018 Jul 10. Available from: https://www.forbes.com/sites/forbestechcouncil/2018/07/10/know-your-customer-kyc-will-be-a-great-thing-when-it-works/?sh=75bf384d8dbb [cited 4 February 2021].
3. U.S. Department of Health and Human Services Food and Drug Administration. Identifying trading partners under the Drug Supply Chain Security Act: guidance for industry – draft guidance. 2017 August. Available from: https://www.fda.gov/files/drugs/published/Identifying-Trading-Partners-Under-the-Drug-Supply-Chain-Security-Act-Guidance-for-Industry.pdf [cited 4 February 2021].
4. U.S. Food and Drug Administration. Drug Supply Chain Security Act law and policies. U.S. Department of Health and Human Services Food and Drug Administration. Available from: https://www.fda.gov/drugs/drug-supply-chain-security-act-dscsa/drug-supply-chain-security-act-law-and-policies [updated 23 October 2020; cited 4 February 2021].
5. Freisleben J. VRS update: Past, present, future. 2018 December 12. In: HAD.org. Arlington, VA: Healthcare Distribution Alliance; 2018. Available from: https://www.hda.org/news/hda-blog/2018/12/07/14/44/2018-12-12-vrs-update-past-present-future [cited 4 February 2021].
6. GS1 Healthcare US. Standard 1.1 – applying the GS1 lightweight messaging standard for DSCSA verification of returned product identifiers. 2020. Available from: https://www.gs1us.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=1897&language=en-US&PortalId=0&TabId=134 [cited 4 February 2021].
7. Jürgens G. Industry-wide DSCSA compliance pilot successfully completed. 2020 December 17. In: Medium.com. Spherity; 2020. Available from: https://medium.com/spherity/industry-wide-dscsa-compliance-pilot-successfully-completed-d7223a0f2c92 [cited 4 February 2021].
8. XATP Working Group. Framework for eXtended ATP authentication, enhanced verification, and saleable returns documentation. Las Vegas, NV: LedgerDomain; 2020 December 17. Available from: https://www.xatp.org/whitepaper [cited 4 February 2021].
9. Chadwick D, Longley D, Sporny M. Verifiable credentials data model 1.0: expressing verifiable information on the web. World Wide Web Consortium (W3C); 2019 November 19. Available from: https://www.w3.org/TR/vc-data-model/ [cited 4 February 2021].
10. GS1 Healthcare US. Assessing current implementation of DSCSA serialization requirements. Ewing, NJ: GS1 US; 2018. Available from: https://www.gs1us.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=1210&language=en-US&PortalId=0&TabId=134 [cited 4 February 2021].
11. Partnership for DSCSA governance. PDG FDA pilot program round-robin webinar series. Partnership for DSCSA Governance (PDG); 30 June 2020. Available from: https://dscsagovernance.org/wp-content/uploads/2020/08/Attachment-A-Presentations.pdf (see slides 16-29) [cited 4 February 2021].
12. U.S. Department of Health and Human Services Food and Drug Administration. Verification systems under the Drug Supply Chain Security Act for certain prescription drugs guidance for industry – draft guidance. 2018 October. Available from: https://www.fda.gov/media/117950/download [cited 4 February 2021].
13. GS1 Healthcare US. Standard 1.2 – applying GS1 standards for DSCSA and traceability. 2016 November 7. Available from: https://www.gs1us.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=749&language=en-US&PortalId=0&TabId=134 [cited 4 February 2021].
14. GS1 Healthcare US. GS1 lightweight messaging standard for verification of product identifiers. 2018 December. Available from: https://www.gs1.org/docs/epc/GS1_Lightweight_Verification_Messaging_Standard.pdf [cited 4 February 2021].
15. U.S. Department of Health and Human Services Food and Drug Administration. Wholesale distributor verification requirement for saleable returned /drug product and dispenser verification requirements when investigating a suspect or illegitimate product – compliance policies: guidance for industry – draft guidance. 2020 October. Available from: https://www.fda.gov/media/131005/download [cited 4 February 2021].
16. U.S. Department of Health and Human Services Food and Drug Administration. DSCSA pilot project program. U.S. Department of Health and Human Services Food and Drug Administration. Available from: https://www.fda.gov/drugs/drug-supply-chain-security-act-dscsa/dscsa-pilot-project-program [updated 22 May 2019; cited 4 February 2021].
17. Chien W, de Jesus J, Taylor B, Dods V, Alekseyev L, Shoda D, et al. The last mile: DSCSA solution through Blockchain Technology: drug tracking, tracing, and verification at the last mile of the pharmaceutical supply chain with BRUINchain. BHTY. 2020 March 12; 3. doi: 10.30953/bhty.v3.134. Available from: https://blockchainhealthcaretoday.com/index.php/journal/article/view/134 [cited 4 February 2021].
18. Androulaki E, Barger A, Bortnikov V, Cachin C, Christidis K, Caro A, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains. Proceedings of EuroSys 2018 conference. 2018. doi: 10.1145/3190508.3190538. Available from: https://arxiv.org/abs/1801.10228 [cited 4 February 2021].
19. Typically used by PICs to authorize pharmacy employees to issue orders for Schedule I and II controlled substances under DEA guidelines, Power of Attorney is increasingly being applied to other regulatory compliance measures. See Gabay M. Federal Controlled Substances Act: ordering and recordkeeping. Hosp Pharm. 2013 December 9; 48(11): 919–21. doi: 10.1310/hpj4811-919. Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3875106/ [cited 4 February 2021].
20. Sourced from National Library of Medicine. DailyMed. Available from: https://dailymed.nlm.nih.gov/dailymed/ [cited 4 February 2021].
21. PharmaCompass. Top 1000 global pharmaceutical companies. LePro PharmaCompass OPC; c2021. Available from: https://www.pharmacompass.com/data-compilation/top-1000-global-pharmaceutical-companies [cited 4 February 2021].
22. Modeled after the regulatory requirement that credit and debit card receipts have truncated account numbers to prevent identity theft. Federal Trade Commission. Federal law requires all businesses to truncate credit card information on receipts. Washington, DC: FTC; 2007 May. Available from: https://www.ftc.gov/tips-advice/business-center/guidance/slip-showing-federal-law-requires-all-businesses-truncate [cited 4 February 2021].
23. Matney L. Apple's global active install base of iPhones surpassed 900 million this quarter. TechCrunch; 2019 January 29. Available from: https://techcrunch.com/2019/01/29/

apples-global-active-install-base-of-iphones-surpassed-900-million-this-quarter/ [cited 4 February 2021].
24. Shuaib K, Saleous H, Shuaib K, Zaki N. Blockchains for secure digitized medicine. J Pers Med. 2019 Jul 13; 9(3): 35. doi: 10.3390/jpm9030035
25. Brook C. What's the cost of a data breach in 2019? 2020 December 1. In DataInsider. Digital Guardian; 2020. Available from: https://digitalguardian.com/blog/whats-cost-data-breach-2019 [cited 4 February 2021].
26. Keen E, Moore S. Gartner forecasts worldwide information security spending to exceed $124 billion in 2019. Sydney: Gartner; 2018 August 15. Available from: https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019 [cited 4 February 2021].
27. Ponemon L. What's new in the 2019 cost of a data breach report. 2019 July 23. In: SecurityIntelligence. IBM Security; 2019. Available from: https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/ [cited 4 February 2021].
28. Steel A. Passwords are still a problem according to the 2019 Verizon data breach investigations report. 2019 May 21. In: LastPass Blog. LastPass; 2019. Available from: http://blog.lastpass.com/2019/05/passwords-still-problem-according-2019-verizon-data-breach-investigations-report/ [cited 4 February 2021].
29. Lu D. How much are password resets costing your company? Okta; 2019 August 20. Available from: https://www.okta.com/blog/2019/08/how-much-are-password-resets-costing-your-company/ [cited 4 February 2021].
30. Bourque A. Ditching passwords and increasing ecommerce conversion rates by 54%. CIO; 2017 May 1; Opinion. Available from: https://www.cio.com/article/3193206/ditching-passwords-and-increasing-ecommerce-conversion-rates-by-54.html [cited 4 February 2021].
31. StClair J, Ingraham A, King D, Marchant MB, McCraw FC, Metcalf D, et al. Blockchain, interoperability, and self-sovereign identity: trust me, it's my data. BHTY. 2020 January 6; 3. doi: 10.30953/bhty.v3.122. Available from: https://blockchainhealthcaretoday.com/index.php/journal/article/view/122 [cited 4 February 2021].