Introducing Privacy Receipts into DLT and eIDAS

Jan Lindquist

Swedish Institute for Standards (SiS), StantICT, Stockholm, Sweden
E-mail: jan@linaltec.com

Received 30 June 2022; Accepted 22 November 2022;
Publication 08 May 2023

Abstract

The introduction of digital identification (e.g., eIDAS) and wallet standards (e.g., EUDI wallet) require compliance with privacy principles and clear communication of the principles through privacy notice and record of consent in the form of a privacy receipt. Regulation needs standards to help set the bar for reducing the privacy infringement risk. Without a standard-based implementation, solutions will be proprietary and siloed with no concern for interoperability, like privacy labels in Google and Apple app stores. Do existing standards address the gap, or do new ones need to be introduced? This article looks at the standards and regulations in three areas to answer this question: privacy protection standards, blockchain and DLT standards, and digital identification and wallet standards.

Keywords: Privacy, GDPR, consent, DLT, blockchain, identity management, eIDAS, digital identity, wallet.

1 Introduction

Services collect massive amounts of personal data on the individual. The privacy policies and cookie banners that should help individuals understand

Journal of ICT Standardization, Vol. 11_2, 117–134.
doi: 10.13052/jicts2245-800X.1121

how their personal data is processed are complex, and very few people take the time to read them. Apple and Google app stores introduced privacy labels to simplify reading the privacy policy. The privacy labels describe through visual icons the type of personal data processed or used for tracking. While privacy labels are an advancement, they can be inaccurate and can consequently be misleading [29].

Many services use federated identity solutions like Google and Facebook to allow individuals to log in. There is limited control over what personally identifiable information (e.g., e-mail and name) is shared. These services may use personally identifiable information to match with personal data collected by data brokers. A privacy policy should explain the type of processing, like matching with external data brokers. The introduction of national digital identity like the EU's digital identity (e.g., eIDAS [5]) will reduce the need for federated identity solutions like Google and Facebook. How will the services adopting national digital identity inform the practice of matching the individual's data? The same risks for matching will continue without a better communication method, like privacy labels.

eIDAS introduces attested attributes which are personal data with a higher level of truth, like a passport or driver's license but in digital form. Attested attributes can be of different types, for example, proof of covid vaccination or, through more advanced techniques, use zero-knowledge-proof (ZKP). ZKP allows for attested attributes to convey proof that an individual is of drinking age without revealing the contents of a driver's license, like a birthday or home address. Attested attributes can be digital certificates, frequently called verifiable credentials. A digital wallet app [17] installed on the phone can carry attested attributes like a regular driver's license but in digital form. While this is a revolution in convenience, the privacy policy associated with sharing the attested attributes does not make it easier to understand the processing of personal data.

The EU is introducing several regulations to help establish a fairer data-sharing ecosystem, for example, Data Governance Act [2], GDPR [3], and ePrivacy [4]. In the Data Governance Act, a consent form shall be established [article 25] but lacks details of the form's content.

Regulation needs standards to help set the bar for reducing the risk of infringement of an individual's privacy rights. Without a standard implementation, the solutions will be proprietary and siloed, with no concern for interoperability. Do existing standards address the gap, or do new ones need to be introduced?

This article looks at the standards and regulations in three areas to try to answer this question. The areas are privacy protection standards, blockchain and DLT standards, and identification and wallet standards. The methodology section sets the requirements for the analysis and discussion sections.

2 Terms, Definitions and Abbreviations

These are some of the terms taken from ISO/IEC 29100 [1] (standard available for free from the ISO portal) and ISO/IEC 27701 [6] to help read the article. The term PII, in the context of this article, refers to personal data and associated attributes.

2.1 Consent

Personally identifiable information (PII) principal's freely given, specific, and informed agreement to the processing of their PII.

2.2 Notice

In the context of this 29100 privacy framework, the term "privacy policy" is used to refer to the internal privacy policy of an organisation. External privacy policies are referred to as notices.

2.3 Personally Identifiable Information (PII)

Any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal.

2.4 Privacy Information Management System (PIMS)

Information security management system which addresses the protection of privacy as potentially affected by the processing of PII.

2.5 Privacy Policy+

Overall intention and direction, rules and commitment, as formally expressed by the personally identifiable information (PII) controller related to the processing of PII in a particular setting.

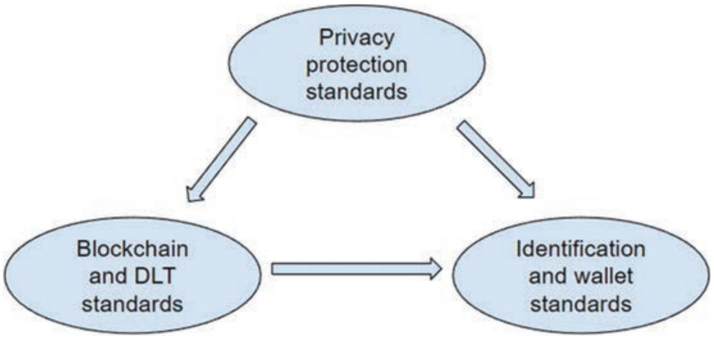
Privacy protection standards
Blockchain and DLT standards
Identification and wallet standards

Figure 1 Privacy protection, blockchain/DLT, and identification/wallet triangle.

2.6 Privacy Receipt (Consent Receipt)

Reference to a consent record that may contain data from the reference consent record.

2.7 Privacy Record (Consent Record)

Information record describing the time and manner of a PII Principal's acceptance of PII processing notice.

3 Methodology

This section sets the method to evaluate how privacy protection standards help communicate with an individual their privacy rights when using blockchain and DLT standards and when adopting new digital identification regulations (e.g., eIDAS [5]) and the new EUDI digital wallet framework [17]. The triangle in Figure 1 helps illustrate the relationship.

To better understand the ISO/IEC privacy standards landscape, the following section breaks down the privacy standards into three layers: framework, management, and implementation.

3.1 Privacy Standards Landscape

The privacy standards described in this section come from the standards subcommittee ISO/IEC JTC 1/SC 27 Working Group 5 Information security, cybersecurity, and privacy protection. These ISO standards are an excellent reference since they reflect international consensus and are independent of regional regulation, e.g., GDPR. The privacy standards can be broken down

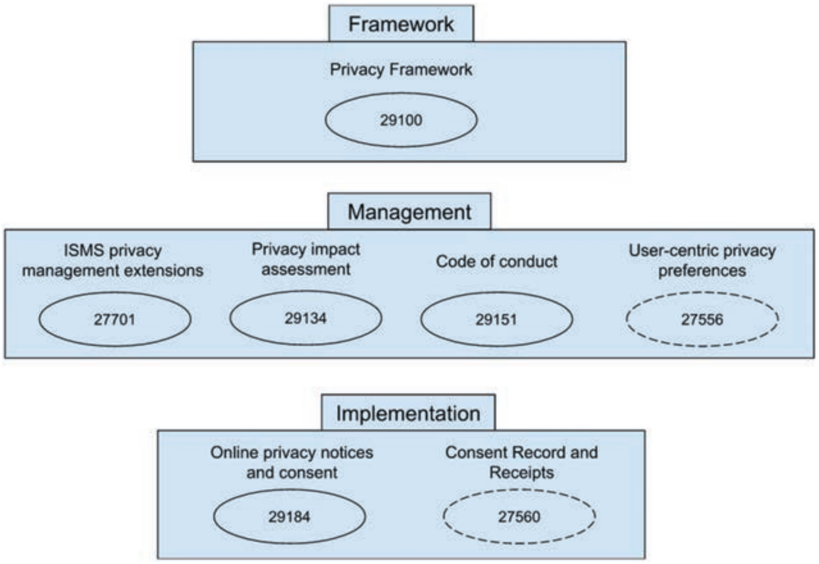
Framework
Privacy Framework
29100
Management
ISMS privacy management extensions
27701
Privacy impact assessment
29134
Code of conduct
29151
User-centric privacy preferences
27556
Implementation
Online privacy notices and consent
29184
Consent Record and Receipts
27560

Figure 2 Overview of the hierarchy of privacy protection standards.

into the framework, management, and implementation layers, as depicted in Figure 2. The referred standards in the figure are not complete but for a comprehensive overview, refer to [28]. The standards with a dashed circle are not published but are in the process of finalization.

The top layer describes the privacy framework (ref ISO/IEC 29100 [1]) and the terminology across the privacy standards. The privacy framework also sets the privacy principles to be followed, which are closely associated with "privacy by design."

The management layer covers standards that help with privacy management: the ISMS privacy management extension (ISO/IEC 27701 [6]), assessment (ISO/IEC 29134 [7]), code of conduct (ISO/IEC 29151 [8]) and user-centric privacy preference management (ISO/IEC FDIS 27556 [9]).

The final layer covers implementation and communication. The focus is on these standards: online privacy notices and consent (ISO/IEC 29184:2020 [10]) and soon to be finalized for publication consent records and receipts (ISO/IEC AWI TS 27560 [11]).

3.2 Privacy Principles

The ISO/IEC 29100 [1] standard provides a high-level framework for protecting personal data or personally identifiable information (PII) as defined in ISO standards. The standard helps specify privacy terminology, actors and roles in processing personal data, privacy safeguards requirements, and reference to privacy principles frequently referred to by management standards. A complete list of the privacy principles is in the requirements Section 3.4.

3.3 Privacy Notice and Receipt

The privacy notice is an extract of the privacy policy but codified using privacy ontology. The data controller manages the privacy notice. When the individual consents to the privacy notice, the data controller creates a record for accountability, and a receipt is provided to the individual, as illustrated in Figure 3. The individual can then use the privacy receipt to track which data controllers or processors have consented to use their personal data and if any third parties also have access. The privacy receipt includes information on how an individual may withdraw the consent.

What is a privacy receipt? The privacy receipt is like a sales receipt from a store. The privacy receipt may be transmitted digitally by e-mail or together with the transfer of personal data.

What is the content of a privacy receipt? A typical privacy receipt may look as illustrated in Figure 4 and be composed of: a heading with the service name, one or more purposes for processing personal data, what personal information (attributed) is in question plus if any of these attributes are optional and do NOT need to be shared if any attributes are sensitive in nature, storage location, retention period, any third parties with access to the personal data and reference to how to exercise privacy rights for example to withdraw consent. The privacy notice may include trust assurance references to adhered code of conduct or identified risks from a privacy assessment, similar to a warning label on a cigarette pack.

Interoperability is essential, as is the ability to automate the processing of the privacy notice and receipt. The same interpretation of the allowed

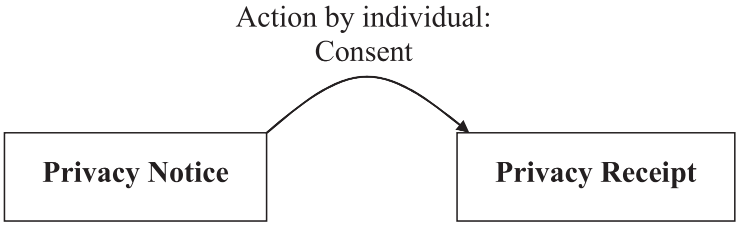

Figure 3 Privacy notice and receipt.

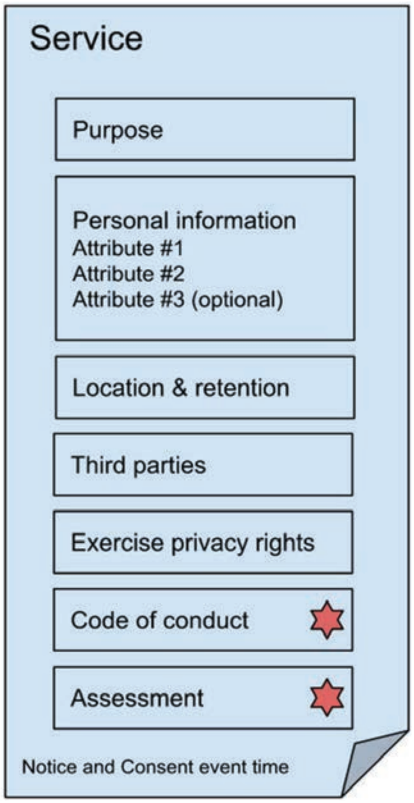

Figure 4 Privacy receipt overview.

values needs to be followed, like purpose types (e.g., marketing, customer care, research) and attribute types (e.g., personal identity, e-mail, health data). For this reason, a privacy ontology is needed, like the W3C Data Privacy Vocabulary and Controls Community Group [Ref. [18, 19]]. By establishing a common vocabulary in the privacy receipts, it is possible to automate decision-making and set up policy access control prohibiting sharing of personal data if violating cross-border data transfer. As standardized in ISO/IEC 27556 [10], user-centric privacy preferences can process machine-readable privacy notices and automate responses.

The ISO/IEC 29184 [10] standard specifies the controls that set the structure of online privacy notices and getting consent. The ISO/IEC 27560 [10] standard defines the structure of a privacy (consent) record and receipt. The standard is similar to the Kantara consent receipt specification [12].

3.4 Requirements

The privacy principles from ISO/IEC 29100 [1] will determine how well a standard considers privacy questions. The communication of privacy principles is central to keeping an individual informed. The support of privacy notice and receipt described in Section 3.3 will be used as a requirement to establish how well a standard communicates the privacy principles. The privacy principles are listed in Table 1 and include a mapping GDPR [3]. The mapping between privacy principles and privacy notice and receipt proposes how they can be associated.

Table 1 Privacy principles and communication with individual

Privacy Principles (29100)	GDPR	Privacy Notice and Receipt
Consent and choice (clause 5.2) Note1	Art.5-1a, Art.7	Privacy notice displays purpose and privacy receipt records choice
Purpose, legitimacy and specification (clause 5.3)	Art.5-1b	Privacy notice includes clear expression of purpose
Collection limitation (clause 5.4)	Art.5-1b	Privacy notice includes an explicit list of personal data to be processed and if mandatory or optional
Data minimization (clause 5.5)	Art.5-1c	Similar to collection limitation plus an indication of the type of processing
Use, retention and disclosure limitation (clause 5.6)	Art.5-1e	Privacy notice indicates retention period for collecting personal data
Accuracy and quality (clause 5.7)	Art.5-1f	Not applicable
Openness, transparency and notice (clause 5.8) Note1	Art.5-1a, Art.12	Support of privacy notice and receipt
Individual participation and access (clause 5.9)	Art.12	Privacy receipts include information on how to exercise privacy rights like withdrawal
Accountability (clause 5.10)	Art.5-2, Art.6	Privacy notice may include information on the result of a privacy assessment (ex. DPIA)
Information security (clause 5.11)	Art.5-1f, Art.32	Privacy notice may include information on the result of a security assessment (ex. DPIA)
Privacy compliance (clause 5.12)	Art.5-2	Privacy notice may include information on the result of a privacy assessment (ex. DPIA)

Note 1: These principles are explicitly referred to by ISO/IEC 29184 [10].

4 Analysis and Results

4.1 Privacy Protection Standards

The following sections analyze the privacy protection standards in the management layer, highlighting clauses relevant to the requirements.

4.1.1 ISO/IEC 27701 (ISMS privacy management extensions or PIMS)

The ISO/IEC 27701 standard defines a Privacy Information Management System (PIMS) without requiring a completely new Management System by extending the requirements specified in Information Security Management System (ISMS) defined in ISO/IEC 27001 [24]. The extension allows for implementing privacy and security controls together or separately.

These are some of the highlights (not all) from ISO/IEC 27701 [6], which detail the need to inform the individual details of the processing of personal data.

- Document information to be provided to the individual regarding the privacy principles defined in ISO/IEC 29100 (clause 7.3.2) [1].
- Record disclosure of personal data to third parties (clause 8.5.3) and notification of disclosure (clause 8.5.4).

4.1.2 ISO/IEC 29134 (Privacy Impact Assessment)

The ISO/IEC 29134 [7] standard is a privacy impact assessment (PIA) similar to a DPIA in the EU. The PIA assesses the risks and potential impacts of processing personal data in an organization. The results of the PIA give stakeholders the necessary mitigation measures to reduce the risks.

The assessment highlights the need to inform individuals about their rights and potential risks. These are some of the highlights from ISO/IEC 29134 [7], which relate to the privacy notice and receipt.

- The data controller explains the notification method of privacy principles, like how an individual gives consent and withdraws consent. (clause 6.3.3, Describe what is being assessed)
- Ensure privacy safeguards are implemented, for example, notification of processing of personal data and ability to access and review (clause 6.4.3, Determining the relevant privacy safeguarding requirements)
- Identified privacy risks may require informing the individual of those risks and indicating corrective measures (clause 6.4.4.1, Privacy risk identification)

4.1.3 ISO/IEC 29151 (Code of conduct)

The ISO/IEC 29151 [7] standard sets the privacy code of conduct and establishes the controls and guidelines to meet the PIA described in the previous section. The code of conduct specifies guidelines based on ISO/IEC 27002 [25].

The code of conduct defined in ISO/IEC 29151 [8] clause A.3, Consent and choice, establishes the need for the individual to exercise meaningful, informed, unambiguous, and freely given consent. The clause includes several implementation guidelines on how to process the consent.

4.1.4 ISO/IEC 27556 (User-centric privacy preferences) [not published]

The ISO/IEC 27556 [9] standard describes a user-centric framework for handling personal data based on privacy preferences in an information and communication technology (ICT) system.

The standard promotes a mechanism to incorporate the individual's privacy principles into a machine-readable format. The privacy notice and receipt address the requirement for a machine-readable format.

4.2 Blockchain and DLT Standards

In DLT systems, there are several privacy considerations, especially considering that storing anything in blockchain (in-ledger) can never be forgotten. The practice in DLT is never to store any sensitive or personal data in the ledger. The following subsections analyze the conformance to the requirements established in the methodology section.

4.2.1 ISO/TS 23244 (DLT privacy protection considerations)

The ISO/TS 23244 [12] standard provides an overview of the privacy principles and personal data protection in blockchain and distributed ledger technologies (DLT) systems.

The focus is on the privacy principles from ISO/IEC 29100 [1] and how they relate to DLT (clause 5.5, Privacy policies). One of the principles sticks out, "Collect, store and notarize the consent and notice of the PII principals/data subjects (Principles 1 and 8)". Another principle worth noting is "Provide openness, transparency and notice, for instance, to notify PII principals/data subjects when their PII is accessed or modified by some person or organization." The standard gives no details on the consent and notice.

Adopting PIMS (ISO/IEC 27701 [6]) sets the governance model needed to keep the individual informed (clause 7.5, PII principal awareness). PIMS ensures that privacy-related events like withdrawal are recorded (clause 7.6, Privacy-related complaint handling).

4.2.2 ISO/TR 23249 (Overview DLT systems for identity management)

The ISO/TR 23249 [14] standard overviews existing DLT systems for identity management. Identity management covers managing identity for individuals and organizations across DLT systems, the interaction of actors, and architecture.

The DLT system Sovrin and Hyperledger Indy (clause 6.6) state the organization can hash consent receipts. The hashed consent receipt creates an immutable record of the agreement between an individual and an organization. The hash of the consent receipt does not reveal any details on the contents of the consent, ensuring privacy. The DLT system gives no additional information about the content of the consent receipt nor how the DLT system addresses the privacy principles.

4.2.3 ISO/DTS 23644 (Trust anchors for DLT-based identity management) [not published]

The ISO/DTS 23644 [15] standard “provides concepts and considerations on the use of trust anchors for systems leveraging blockchain and distributed ledger technologies (DLT) for identity management, i.e., the mechanism by which one or more entities can create, be given, modify, use and revoke a set of identity attributes.”

Implementing DLT for identity management offers the option for fine-grained consent management backed by a complete audit trail (clause 6.8). The standards give no additional detail on how the DLT system can support the audit trail.

4.2.4 ISO/IEC 23635 (Blockchain and DLT – Guidelines for Governance)

The ISO/TS 23635 [16] standard provides guiding principles and a framework for the governance of DLT systems.

The standard includes a section on privacy considerations (clause 9.3.3 Privacy) which lists the privacy principles from ISO/IEC 29100. Additional guidance to adhere to the principles is pointed at ISO/TR 23244 previously analyzed.

4.2.5 Other

Other standards have been briefly analyzed but did not provide any context to the requirements in this paper. One of these standards is the ETSI Industry Specification Group (ISG) [26].

ISG sets the foundation for the operation of permissioned distributed ledgers and the creation of smart contracts. When reviewing the standards from ISG, no requirements could be identified relating to privacy principles and privacy notice and consent.

4.3 Identification Management and Wallets

There are many identity management standards, but the article focuses on the EU and the work to create a wallet framework to carry a digital identity. The following subsections analyze the conformance to the requirements established in the methodology section.

4.3.1 eIDAS

The European Digital Identity (eIDAS) [5] standard establishes a framework for a European digital identity.

Reviewing the standard reveals it has no consideration for privacy principles and only establishes the creation of "attested attributes." The attested attributes are personal data with a higher level of truth, like a passport or driver's license, but in digital form. The individual's identity may be pseudonymized and, if so, should be indicated (annex V bullet c), but no explanation of how a system conveys this indication.

eIDAS Annex V bullet 3 specifies that "the attested attribute or attributes, including, where applicable, the information necessary to identify the scope of those attributes." The bullet is unclear what is meant by scope. It could be related to the privacy notice, but it is unclear.

4.3.2 EUDI Wallet

The EUDI Wallet is a reference framework for a European Digital Identity architecture [17]. A clear set of requirements are set on the user interface for users to be aware of (clause 4.6.1 User awareness component). These are some of the highlights associated with privacy principles.

- attestation of attributes, including who is asking, which attributes are requested, and for which purpose, as defined by the relying party,
- clearly informed of the type of operation being executed,
- her/his rights for data protection under the GDPR,

- display an "EU Digital Identity Wallet trust mark" for the user,
- restrict sharing certain sets of attributes with certain parties, or warn the user that the relying party may not be authorized to use/ask for these attributes.

The wallet framework sets the expectations but does not entirely address how the wallet shall convey the information. Further details are needed to establish a standard means of providing a privacy notice. The privacy notice is displayed when the individual is requested to share their digital identity and associated attested attributes from the wallet.

4.3.3 Other

Other standards have been briefly investigated but did not provide any context to the requirements in this paper. One of these standards is the ETSI TC ESI [24].

ESI is responsible for Electronic Signatures and infrastructure standardization within ETSI. The focus is on identity proofing. When reviewing the standards from ESI, no requirements could be identified relating to privacy principles and privacy notice and consent.

5 Discussion

When implementing blockchain and DLT standards, ISO/TR 23244 analyzes the privacy principles and guides adherence to ISO/IEC 29100. The privacy policies clause states the need to notarize notice and consent and to provide transparency when a modification to the policy occurs (clause 5.5). When establishing a DLT system, PIMS should consider how to handle privacy-related complaints (clause 7.6).

The DLT- based identity management [14] suggests fine-grained consent management as a means of improving the audit trail but no details on the content of the consent receipt nor how the DLT system addresses the privacy principles. There are industry forums that have been prototyping and developing a means of conveying a notice and consent in DLT systems through credentials or as part of an exchange of verifiable credentials and presentation proofs (refer to Hyperledger [20], NGI eSSIF-labs [21], DIF data agreements [22]). The work helps establish reference implementation in DLT with the ambition to achieve interoperability between organizations.

With the introduction of a new digital identity, eIDAS seems to miss adherence to any privacy principles completely. The EUDI wallet [17] suggests some privacy principles but is incomplete. It does not refer to any standard or mechanism to convey the information, which makes it hard to check conformance. Taking some of the guidelines stipulated by ISO/TS 23244 [13], DLT privacy protection considerations may help be more systematic in setting the conformance.

None of the covered standards describe the content of the notice, which raises concern that there is no systematic approach to keep the individual informed nor an audit trail that can span across data controllers, data processors, and third parties. A new standard or guidance that bridges the privacy principles and privacy notice/receipt proposed in this article with the digital identity and attested attributes. DLT standards provide good input for guidance on the privacy principles but lack the privacy notice/receipt details.

The lesson learned from cookies is that automation is mandatory to process the privacy notice against privacy preferences [9] without requiring explicit consent. Users are suffering from cookie banner fatigue. The individual's privacy preferences can set policies that indicate which purposes are acceptable and which are not. The user-centric control of these policies has been demonstrated on SOLID pods [23] using privacy ontology from W3C Data Privacy Vocabulary [18]. Before automated consent is supported, there needs to be support for a standardized privacy notice and receipt.

6 Conclusion

Privacy labels used by Apple and Google app stores are a step forward in communicating the privacy policy more concisely with simple icons representing different data types. The app store can then systematically display the privacy labels for all apps. Unfortunately, these privacy labels supported by Google and Apple are proprietary, and each has its flavor and lacks a single standard. Support for privacy notices and receipts standards is required (i.e., ISO/IEC 29184 [10], ISO/IEC 27560 [11], and Kantara Consent Receipt specification [12]). The privacy notice and receipt described in Section 3.3 allows for interoperability and automation, reducing the burden on the individual.

The EUDI wallet lacks a standard means of providing privacy notices with information stipulated in the user awareness component clause 4.6.1 [17]. The entity (e.g., data controller or processor) requesting access to content in the wallet should display the requested attested attribute(s) along with the privacy notice. Once individual consents to sharing data, a privacy receipt is generated and can be stored in the wallet for traceability purposes.

The conclusion is that a new standard is required to guide eIDAS and EUDI to adopt privacy notices and receipts. The new standard's outcome is to systematically review the adoption of the privacy principles and add relevant guidance to support privacy notice and receipt standards. One of the DLT standards, ISO/TS 23244 [13], provides some guidance in the review of privacy principles. Once privacy notice and receipts standards are adopted, it is possible to go to the next level with user privacy preferences and consent automation. Consent automation would come a long way to help address the indifference to cooky banners and hard-to-read privacy policies.

Acknowledgments

Special thanks to Arianna Rossi at UNIVERSITÉ DU LUXEMBOURG and Harshvardhan J. Pandit at ADAPT Centre, Dublin City University, for being a discussion partners in writing the article.

References

[1] ISO/IEC 29100:2011. Information technology – Security techniques – Privacy Framework https://www.iso.org/standard/45123.html

[2] Data Governance Act. https://www.consilium.europa.eu/en/press/press-releases/2022/05/16/le-conseil-approuve-l-acte-sur-la-gouvernance-des-donnees/

[3] GDPR. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) https://eur-lex.europa.eu/eli/reg/2016/679/oj

[4] ePrivacy. REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52017PC0010

[5] eIDAS. REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity https:

//eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0281&from=EN

[6] ISO/IEC 27701:2019. Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines https://www.iso.org/standard/71670.html

[7] ISO/IEC 29134:2017. Information technology – Security techniques – Guidelines for privacy impact assessment https://www.iso.org/standard/62289.html

[8] ISO/IEC 29151:2017. Information technology – Security techniques – Code of practice for personally identifiable information protection https://www.iso.org/standard/62726.html

[9] ISO/IEC FDIS 27556. Information security, cybersecurity and privacy protection – User-centric privacy preferences management framework https://www.iso.org/standard/71674.html

[10] ISO/IEC 29184:2020. Information technology – Online privacy notices and consent https://www.iso.org/standard/70331.html

[11] ISO/IEC AWI TS 27560. Privacy technologies – Consent record information structure https://www.iso.org/standard/80392.html

[12] Consent Receipt Specification 1.1.0, published December 30, 2019 https://kantarainitiative.org/download/7902/

[13] ISO/TR 23244:2020. Blockchain and distributed ledger technologies – Privacy and personally identifiable information protection considerations https://www.iso.org/standard/75061.html

[14] ISO/TR 23249:2022. Blockchain and distributed ledger technologies – Overview of existing DLT systems for identity management https://www.iso.org/standard/80805.html

[15] ISO/DTR 23644. Blockchain and distributed ledger technologies – Overview of trust anchors for DLT-based identity management (TADIM) https://www.iso.org/standard/81773.html

[16] ISO/TS 23635:2022. Blockchain and Distributed Ledger Technologies – Guidelines for Governance https://www.iso.org/standard/76480.html

[17] European Digital Identity Architecture and Reference Framework – Outline, published February 22, 2022 https://ec.europa.eu/newsroom/dae/redirection/document/83643

[18] W3C Data Privacy Vocabulary (DPV) https://w3c.github.io/dpv/dpv/

[19] Creating a Vocabulary for Data Privacy, The First-Year Report of Data Privacy Vocabularies and Controls Community Group (DPVCG) Harshvardhan J. Pandit, Axel Polleres, Bert Bos, Rob Brennan, Bud Bruegger, Fajar J. Ekaputra, Javier D. Fernández, Roghaiyeh Gachpaz

Hamed, Elmar Kiesling, Mark Lizar, Eva Schlehahn, Simon Steyskal & Rigo Wenning https://link.springer.com/chapter/10.1007/978-3-030-33246-4_44

[20] Hyperledger Aries RFC 0167: Data Consent Lifecycle https://github.com/hyperledger/aries-rfcs/tree/main/concepts/0167-data-consent-lifecycle

[21] NGI essif-lab ioc, Automated Data Agreements https://www.ngi.eu/funded_solution/essif-ioc-30/

[22] DIF Claims & Credentials – data agreement work item https://github.com/decentralized-identity/data-agreement

[23] COnSeNT 2021 – ODRL Profile for Expressing Consent through Granular Access Control Policies in Solid, Beatriz Esteves https://www.slideshare.net/BeatrizEsteves23/consent-2021-odrl-profile-for-expressing-consent-through-granular-access-control-policies-in-solid

[24] ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements https://www.iso.org/standard/54534.html

[25] ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection – Information security controls https://www.iso.org/standard/75652.html

[26] ETSI Electronic Signatures and Infrastructures Activities https://portal.etsi.org/TB-SiteMap/esi/esi-activities

[27] ISG PDL activity report 2021 https://www.etsi.org/committee-activity/activity-report-pdl

[28] ISO/IEC JTC 1/SC 27/WG 5 “Identity management and privacy technologies” – WG5 SD1 Roadmap https://www.din.de/resource/blob/259644/c0aa4373b3c56277cab61cd15b5f1368/sc27wg5-sd1-data.pdf

[29] Mobile-App Privacy Nutrition Labels Missing Key Ingredients for SuccessBy Lorrie Faith CranorCommunications of the ACM, November 2022, Vol. 65 No. 11, Pages 26–28 https://cacm.acm.org/magazines/2022/11/265814-mobile-app-privacy-nutrition-labels-missing-key-ingredients-for-success/fulltext

Biography

Jan Lindquist received a bachelor's degree in electrical engineering from the Illinois Institute of Technology in 1991. He is currently a member of the Swedish Institute for Standards (SiS) and co-editor of the ISO/IEC 27560 standard with a long history of standardization work across multiple sectors. He performs data protection impact assessments to help organizations adhere to GDPR and information security requirements. He is engaged in various NGI-awarded (eSSIF-labs and ONTOCHAIN) collaborations to develop interoperable privacy receipts. He also helped lead working groups in the decentralized identity foundation (DIF) to create an open-source solution based on DID method.