Government-Issued Digital Credentials and the Privacy Landscape

2 April 2023
Version: Draft for Public Comment
Lead Editor: Heather Flanagan

Table of Contents

Contributors

Multiple non-profits have made this paper possible, for which we offer great thanks. The formal use of their names will be subject to their internal governance processes and will be published in the final publication of this paper.

In addition, this paper could not exist without the support of several individuals that offered their time and knowledge to inform the content and themes included here.

- Dr Joseph Atick, ID4Africa
- Vittorio Bertocci, Okta, Inc.
- Debora Comparin, Thales DIS
- Bill Nelson, Identity Fusion, Inc.
- Gail Hodges, Executive Director, OpenID Foundation
- Mike Kiser, SailPoint Technologies
- Stephanie de Labriolle, Executive Director, Secure Identity Alliance (SIA)
- Giuseppe De Marco, Dipartimento per la trasformazione digitale
- Rachelle Sellung, Fraunhofer Institute
- Kristel Teyras, Thales DIS
- John Wunderlich, Chair, Kantara Privacy Enhancing Mobile Credential Work Group

1 Executive Summary

Governments around the world are embracing the phrase “digital identity.” As the source for truth for a wealth of personal data (e.g., legal names, dates of birth, citizenship), governments are in a position to improve trust in online and in-person services by issuing digital identity credentials to their citizens and residents and establishing the ground rules for businesses and government agencies to properly use those credentials.

The digital identity landscape for government-issued credentials involves trust, both technical and societal, in several dimensions. Governments cannot act alone in developing a robust, privacy-preserving digital ecosystem. They must work with technologists and civil society conversant with privacy concerns and technological possibilities. And, of course, they must work with their citizens and residents to ensure their needs and expectations are met when it comes to the privacy implications of an increasingly digitally focused world.

This paper offers a sampling of where and how government-issued digital credentials are used, what standards and regulations support them, and where urgent work still needs to be done to live up to the promises of a safer, more efficient world. It is intended for government policymakers, civil society members, and technologists so that each group gains a better understanding of what is happening outside their particular silos.

There are several recommendations provided. We start by recommending improvements around the security and privacy posture of the systems involved in the issuance, storage, verification, and use of government-issued digital credentials. There are several excellent resources to guide governments and services towards better data hygiene such as NIST Cybersecurity Framework and the proposed EU Cyber Resilience Act. Managing the basics, however, falls in the “necessary but not sufficient” category. There must also be a recognition of ongoing concerns around surveillance, the challenges of diversity, equity, and inclusion, the grey areas of legality, and the sustainability of legal protections in the face of changing administrations.

With new technologies come new concerns, and this is true for digital identity credentials as well. An increased dependency on them provides another vector for attack during digital warfare. Deepfakes also add new threats to the ability to verify remote use of credentials; it is an example of one entry in a digital arms race.

In all cases, governments, technologists, and civil society members must keep in mind the reality of what is reasonable to expect from the individuals participating (or not) in this ecosystem. Individuals must be offered choices, but those choices should in turn be clear, actionable, and straightforward, with protecting the privacy of their data being the easiest option.

Ultimately, the goal of this paper is to engage and inspire a community of thought leaders to come together to develop a path forward for government-issued digital identity credentials. We must work together to close the policy and protocol gaps that exist between today's reality and the goal of a privacy-preserving, globally and at Internet-scale.

2 Intro / Scope

Governments around the world are moving towards issuing digital credentials to their citizens and registered residents; sometimes slowly in various pilot phases, other times as a well-funded mandate that is already becoming ubiquitous in local populations. Individuals are growing to expect the level of convenience and control in having everything they need on their mobile devices, and governments are finding that technology allows them to be more efficient and responsive to the needs of their citizens, residents, businesses, and themselves. Organizations in the private sector are also considering how to take advantage of these new credentials. The credentials have an inherently higher value, thanks to required identity assurance levels, but come with privacy risks as businesses consider what it means to balance the need to know their customers with the risk of knowing too much and being held accountable for that data.

Digital credentials, at their most general, are digital files containing information about an individual. When created in accordance with various standards as mentioned in this paper, they are designed to be tamper-proof and allow an individual to choose what information they disclose to services requesting data included in that credential.

In the initial stages, government-issued digital credentials often take the form of digitizing existing physical credentials like transit cards, vaccination records, and driver's licenses. But with the promise of more—more features, more data, more utility—the relatively simple digitized replicas are moving towards pure digital credentials (i.e., credentials that do not have a physical analog and exist only in electronic records). The World Bank describes the evolution this way: "As societies become more digital, we have begun to see a move toward

digital-only ID systems that do not rely on the possession of a physical credential."[1] Digital credentials offer a more dynamic set of information, easily updated and expanded to meet the needs of the moment. With so much data becoming readily available, it is an understandable next step to use that data in new and creative ways, with increasing implications for individual privacy.

Government stakeholders are keenly feeling the privacy implications around the digital economy in general, and more recently around government-issued digital credentials specifically. Governments themselves are looking for ways to establish effective privacy legislation while taking into consideration matters of public safety. Well-publicized data breaches in both the government and private sectors leave individuals and members of civil society deeply concerned about the risk of their personal information being exposed.[2] Equally, there is the concern that the government will use the personal data they hold in combination with new data they collect about where, when, and how government-issued credentials are used as a means of surveillance. As a result, privacy advocates and everyday people react strongly and negatively when taken by surprise at the perceived expansive scope of how government agencies and third parties may use these new credentials in their lives.

What is often missing from the conversation, however, is that no single party involved in an identity ecosystem, including governments, should be fully trusted when it comes to individual data. While it is true that government-issued credentials have special privacy considerations due to their inclusion of verified personal data, the literature in this space often overlooks that identity systems are, at minimum, a multi-way trust model. Privacy requirements exist between the credential issuer (in our case, the government), the credential consumer (such a governmental agency, private business, or another individual), the device and app or wallet holding the credential, and the individual.

In addition to the considerations of governance, there are the complications coming from the technological complexity and myriad implementations. The concerns that civil society

[1] "Types of Credentials and Authenticators | Identification for Development," Accessed April 2, 2023. https://id4d.worldbank.org/guide/types-credentials-and-authenticators.

[2] See for example media reports on the 2018 Aadhaar breach (Sapkale, Yogesh. "Aadhaar Data Breach Largest in the World, Says WEF's Global Risk Report and Avast." Moneylife NEWS & VIEWS, February 19, 2019. Accessed April 1, 2023. https://www.moneylife.in/article/aadhaar-data-breach-largest-in-the-world-says-wefs-global-risk-report-and-avast/56384.html) and reports on various U.S. government breaches (Lord, Nate. "Top 10 Biggest Government Data Breaches of All Time in the U.S." Digital Guardian, October 6, 2020. Accessed April 1, 2023. https://www.digitalguardian.com/blog/top-10-biggest-us-government-data-breaches-all-time).

brings to the table about the potential for government surveillance and for private entity misuse of data further establishes that no one component can be trusted on its own.

Beyond the need for multi-party trust models that can work within and across jurisdictions, there is the issue of user experience itself. The design of each user flow can itself help users make wise and privacy preserving choices, or mislead users and undermine those choices. The gaps between the technological realities of what is possible with technology today, the privacy demands in legislation and regulation, and government requirements for verified identities are wide and yet, are often lost in the complexity of the digital ecosystem by the stakeholders focused on their pieces of the puzzle.

This whitepaper is focused on the privacy implications surrounding government-issued digital credentials. In particular, we look at the digital credentials issued by government authorities and intended as a technology that helps enable efficient, privacy-preserving services to people and businesses. Similarly, we consider where legislation and regulation define the individual's expectation for privacy and establish some of the requirements for the technology. The scope here is global, with a particular focus specifically on digital credentials issued by liberal democratic governments which tend to have more stringent privacy laws and higher expectations of their residents to have their privacy expectations met. The paper does not cover privately issued identity credentials, what governments need to do to provide services to users that do not have government issued identity credentials, or the needs of centralized governments with less focus on privacy.

To understand what it will take to get to a more privacy-preserving future for government-issued digital identity credentials, we first have to understand the landscape today. In "Getting There from Here," we'll take a look at the current privacy landscape and the state of government-issued and associated derived credentials in several countries and localities around the world. We'll also consider the key issues being encountered with biometrics, data minimization, privacy legislation, user control, and relying party reliability and accountability. The digital transformation underway offers several promises to improve individual privacy and the usability of digital credentials, and we'll review what promises are being made and to whom.

Providing digital credentials to individuals opens the door to a world of potential, but there are many gaps and risks involved in the journey. In the section "Gaps and Risks," we'll look at what it will take to fulfill those promises at Internet scale. From policy considerations to protocol changes, there are no silver bullets to meeting the needs of all the stakeholders

involved, but there are positive steps that both policy-makers and civil society can make to move towards a more privacy-respecting future.

3 The Current Landscape of Policy and Technology

To say the current privacy landscape is complicated understates the diversity of challenges in this space. What we are seeing in terms of tension expressed in the news and lawsuits in court reflects an unsteady balance between privacy and desired functionality that varies from one jurisdiction to the next. Every locality makes different decisions depending on its capabilities and understanding of what it means to issue and use digital credentials in a privacy-respecting manner. In the larger use cases, mobile driver's licenses being the primary example, discussions start with looking at what's possible with the physical credentials today. Photographs and physical characteristics (biometrics), counterfeit protection (issuer verifiability), name and address (individual identifiers), and so on, start as the bare minimum of what digital credentials are expected to offer. That they are digital suggests ways in which they can do more to protect an individual's privacy when using the credential.

Even that bare minimum, though, introduces key issues that must be addressed. Providing digital credentials often promises improvements on the physical credentials provided today, but the key issues suggest it's not that easy.

For many organizations, the level of assurance regarding an individual's data that comes from a government-issued digital credential is foundational to their services. When an organization is held to specific legal requirements, such as assessing minimum age or residency , these credentials are the most valuable and perhaps only viable option. Even for unregulated use cases, the default is often for businesses to request user's present government issued identity documents.[3]

In a paper-based environment, however, ascertaining such specific data is a fairly heavy-weight mechanism that reveals far more than just the data actually required for the

[3] "Should I Give My ID to a Dating Website/App? | PrivacyRights.Org," February 10, 2020. Accessed April 1, 2023. https://privacyrights.org/resources/should-i-give-my-id-dating-websiteapp.

situation. Verifying that an individual is of legal age to purchase cigarettes includes not only a specific date of birth, but also a legal name, address, and a government-issued identifier like a social security or driver's license number. The system supports little in the way of privacy and is demonstrably prone to fraud.[4] Still, those weaknesses are understood, whereas the new risks and challenges posed by digital credentials are just starting to register as topics to consider.[5]

With the trend towards digital credentials, governments and services dependent on government data have powerful options to support a more privacy-enhancing landscape for individuals. We will start by looking at the current state of government-issued digital credentials and the characteristics that can make them a better option for all the stakeholders involved. From there we will consider the technology that enables these digital credentials today and how privacy challenges are also likely to evolve in the new landscape.

3.1 Influential National and International Regulations and Standards

The technologies required to support the issuance, maintenance, and handling of digital credentials are shaped by the legal requirements prescribing appropriate use. Many countries and regions are developing their own legal frameworks to address how governments may issue and consume digital credentials, with the European Union's General Data Protection Regulation (GDPR) and the second version of the Network Information Security (NIS2) directive serving as the gold standard for the world, despite ongoing criticism that they do not go far enough in protecting human rights and privacy.[6] Similarly, in the U.S., the California Consumer Privacy Act (CCPA) provides a strong model for other states in the US. Bridging the gaps from one country to another are the Privacy Principles developed and adopted by the Organisation for Economic Co-operation and Development (OECD).

[4] "LexisNexis Risk Solutions. "The True Cost of FraudTM Study | LexisNexis Risk Solutions," 2022. Accessed April 1, 2023. https://risk.lexisnexis.com/insights-resources/research/us-ca-true-cost-of-fraud-study.

[5] Privacy International. "Digital National ID Systems: Ways, Shapes and Forms," October 26, 2021. Accessed April 1, 2023. https://privacyinternational.org/long-read/4656/digital-national-id-systems-ways-shapes-and-forms.

[6] Vanberg, Aysem Diker. "Informational Privacy Post GDPR – End of the Road or the Start of a Long Journey?" The International Journal of Human Rights 25, no. 1 (January 2, 2021): 52–78. https://doi.org/10.1080/13642987.2020.1789109.

All regulations that touch on digital identity and associated credentials require careful reading, as their scope is often (but not always) limited to organizations in the private sector.

3.1.1 OECD Privacy Principles

The OECD Privacy Principles provide a framework for privacy laws around the world. These principles are part of the OECD Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.[7] Having a common set of principles makes international transactions involving personal data much more straightforward as the laws are more likely to be interoperable. These principles are not restricted to government-issued digital credentials, and yet their use guides what is considered best practice in the privacy space.

The Privacy Principles touch on eight areas:[8]

1. Collection Limitation Principle
2. Data Quality Principle
3. Purpose Specification Principle
4. Use Limitation Principle
5. Security Safeguards Principle
6. Openness Principle
7. Individual Participation Principle
8. Accountability Principle

These principles have influenced many critical privacy laws and regulations around the world. For example, these principles are directly reflected in ISO/IEC 29001 Privacy Framework.[9]

[7] OECD. "Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data." OECD Legal Instruments, October 7, 2013. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188.

[8] See Appendix A for the specific text of these principles.

[9] Details regarding the impact of the OECD Privacy Guidelines are available in a recently declassified report: OECD Council. "Report On The Implementation Of The Recommendation Of The Council Concerning Guidelines Governing The Protection Of Privacy And Transborder Flows Of Personal Data: (Note by the Secretary-General)," March 17, 2021. https://one.oecd.org/document/C(2021)42/en/pdf.

3.1.2 ISO/IEC 29100 Privacy Framework

The ISO/IEC 29001 Privacy Framework is a joint standard published by ISO (*the International Organization for Standardization*) and IEC (the International Electrotechnical Commission).[10] This standard serves as the privacy baseline for several other standards and their relevant certifications such as ISO/IEC 27018 for cloud providers and ISO/IEC 27701, an extension to the famous information security management standards, ISO/IEC 27001 and 27002.[11]

Organizations that can demonstrate compliance with ISO/IEC 27701, and therefore follow the guidance in ISO/IEC 29001, are much closer to meeting legal and regulatory requirements around the world. The open-sourced Data Protection Mapping Project, initially donated by Microsoft to the open-source community, exists to help organizations understand how these standards relate to the different data protection regulations around the world.[12]

For service providers looking to take advantage of government-issued digital credentials across several jurisdictions, this kind of standardized guidance is critical.

3.1.3 General Data Protection Regulation

We cannot understate the influence the GDPR has had on the world stage. In effect since 2018, the regulation continues to drive digital identity and privacy policies well beyond the European Union. For a country to receive the economic benefits of being a strong partner to European businesses, it must have adequate data protection regulations as determined by the European Commission.[13] And so, thanks to the "adequacy" requirements for partner

[10] ISO/IEC 29100:2011 Information technology — Security techniques — Privacy framework. ISO/IEC JTC 1/SC 27. Geneva, Switzerland: ISO, published December 2011, reviewed and confirmed in 2017. https://www.iso.org/standard/45123.html.

[11] ISO/IEC 27018:2019 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processor. ISO/IEC JTC 1/SC 27. Geneva, Switzerland: ISO, published January 2019. https://www.iso.org/standard/76559.html and ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines. ISO/IEC JTC 1/SC 27. Geneva, Switzerland: ISO, published August 2019. https://www.iso.org/standard/71670.html.

[12] "GitHub - Microsoft/Data-Protection-Mapping-Project: Open Source Data Protection/Privacy Regulatory Mapping Project." GitHub, last updated on July 26, 2022. Accessed April 1, 2023. https://github.com/microsoft/data-protection-mapping-project.

[13] European Commission. "Adequacy Decisions: How the EU Determines If a Non-EU Country Has an Adequate Level of Data Protection." Accessed April 1, 2023. https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

nations and broad private-sector compliance for organizations needing to operate in a manner to include EU Member State citizens and residents, the GDPR is seen a baseline for data privacy.[14]

The GDPR offers a data-centric approach to security and privacy. With the best intentions, the GDPR creates many obstacles around the sharing of data, a characteristic often considered a positive for commerce but negatively impacting areas such as research and small business.[15] In practice, the only legally viable reason to move data involves the free and informed consent, a fact that leads to the work underway in eIDAS 2.0 (see Section 3.2.4. eIDAS 2.0 (electronic IDentification, Authentication, and trust Services)). The GDPR has been a paradigm shift when it comes to giving individuals agency over their own data, a fact that has significant implications for how digital credentials, including government-issued digital identity credentials, are used.

In those countries where privacy regulation is still in its infancy and the digital economy is only beginning to launch, the GDPR adequacy requirements offer a clear roadmap for how to advance local digital economies in ways that will pave the way for strong partnerships with the EU. With these partnerships comes a hope for economic growth, a powerful motivation to follow the European models of privacy, data handling, and digital credentials. In some ways, it is more difficult for countries with strong, established economies and their own views on citizen and consumer privacy to follow the direction offered by the GDPR.

3.1.4 NIS2 Directive

Whereas the GDPR focuses on data-centric security, the EU's NIS2 Directive focuses on system-level security. Protections for critical infrastructure, a classification that includes the government-issued digital credential systems, will result in additional privacy enhancements for individuals, though privacy is only one of several considerations for the directive. The requirements to secure data implicitly supports privacy for citizens and

[14] Peukert, Christian, Stefan Bechtold, Michail Batikas, and Tobias Kretschmer. "Regulatory Spillovers and Data Governance: Evidence from the GDPR." Marketing Science 41, no. 4 (July 1, 2022): 318–40. https://doi.org/10.1287/mksc.2021.1339.

[15] See for example Clarke, Niamh, Gillian L. Vale, Emer P. Reeves, Mary Kirwan, David Smith, Michael Farrell, G. A. Hurl, and Noel G. McElvaney. "GDPR: An Impediment to Research?" Irish Journal of Medical Science 188, no. 4 (February 8, 2019): 1129–35. https://doi.org/10.1007/s11845-019-01980-2 and Geradin, Damien, Theano Karanikioti, and Dimitrios Katsifis. "GDPR Myopia: How a Well-Intended Regulation Ended up Favouring Large Online Platforms - the Case of Ad Tech." European Competition Journal 17, no. 1 (January 2, 2021): 47–92. https://doi.org/10.1080/17441056.2020.1848059.

residents by mandating specific protections for their data and notification if that data is accessed inappropriately. The directive went into force on 16 January 2023; EU member states must develop appropriate local laws in support of NIS2 by 18 October 2024.[16]

As with the GDPR, while the directive is part of the EU legislative framework, it still has a significant impact on international businesses. If a qualifying business has their primary cybersecurity decision-making point in the EU, they must abide by the requirements of the directive.[17]

3.1.5 SDGR and the Once-Only principle

The Single Digital Gateway Regulation (SDGR) is a regulation that requires, as stated in article 6, that EU countries must provide twenty-one cross-border services online by December 2023 (The European Parliament, 2018).[18] The SDGR states that digital public services should not only be accessible to domestic citizens but also EU citizens, thus encouraging the development of cross-border public services. One of the Single Digital Gateway's priorities consists in encouraging European administrations to implement the Once-Only Principle (OOP) in their approach.[19] This legal framework and services provided by the SDGR binds the EU28 to develop cross-border solutions in a more structured and collaborative way. By the end of 2023, there should be 21 online procedures that should become fully digitalized and eliminate paperwork. The services are related to various life events like birth, residence, studying, working, moving, retiring, and managing a business.

[16] "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive)." European Union, December 14, 2020. http://data.europa.eu/eli/dir/2022/2555/oj.

[17] Vladimirova-Kryukova, Anna. "The Influence of the NIS2 Directive In and Outside of the EU." ISACA NOW BLOG, November 10, 2021. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/the-influence-of-the-nis2-directive-in-and-outside-of-the-eu.

[18] European Commission. "Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 Establishing a Single Digital Gateway to Provide Access to Information, to Procedures and to Assistance and Problem-Solving Services and Amending Regulation (EU) No 1024/2012 (Text with EEA Relevance.)." European Commission, November 21, 2018. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2018.295.01.0001.01.ENG.

[19] European Commission. "Commission Implementing Regulation (EU) 2022/1463 of 5 August 2022 Setting out Technical and Operational Specifications of the Technical System for the Cross-Border Automated Exchange of Evidence and Application of the 'Once-Only' Principle in Accordance with Regulation (EU) 2018/1724 of the European Parliament and of the Council (Text with EEA Relevance)," August 5, 2022. https://eur-lex.europa.eu/eli/reg_impl/2022/1463/oj.

Data minimization in general is an important characteristic for services interested in protecting the privacy of the individuals using their systems. This is equally true for government services, which must follow a difficult line of only requiring the minimum amount of data necessary to use their services when they are the natural source of truth for so much more.

In article 42 of the SDGR it states how the Regulation and the OOP should comply with all of the data protection rules. It specifically identifies the following principles: data minimization, accuracy, storage limitation, integrity and confidentiality, necessity, proportionality, and purpose limitation. It also highlights that the implementation of the regulation should comply fully with “principles of security by design and of privacy by design, and should also respect the fundamental rights of individuals, including those related to fairness and transparency”.

Within the EU, understanding of the OOP varies. In some countries, the OOP is understood in legislation that there is existing only original data with no duplication in other databases, while in other countries the OOP is understood that data is provided only once by citizens or businesses. In the EU framework, the OOP means that a citizen does not have to constantly provide his basic data if they had already provided once to the government entities. The OOP states that a citizen does not have to constantly provide his standard information before using a digitalized public service by allowing public administrations to share his data. In addition, there is an article that highlights how it should minimize the amount of data exchanged to only the specific data that is requested.

3.2 Government-Issued Digital Credential Systems

There are a variety of use cases driving governments to issue digital credentials. From digital national insurance cards to mobile driver’s licenses, countries around the world are exploring ways to make data more current, convenient, and less susceptible to fraud.

While many countries are including privacy principles in their regulations and services, privacy is only one of many considerations for these new systems. The more immediate motivations for issuing government digital identity credentials include:

- helping people to assert their identity more easily online and in person (e.g., open a bank account, purchase age-restricted goods, assert rights to access government benefits, travel with more ease),
- control fraud (e.g., illegal collection of benefits, submitting fake credentials to open financial accounts),
- helping people assert their right to age restricted products or gain access to other services, and
- ease of travel.

The interesting challenge is that governments are simultaneously the credential issuer, consumer, and regulator. The government is issuing the credential for economy-wide use, they are consuming digital identity credentials to ensure an individual's right to access benefits, and they are regulating their own use. These perspectives are complicated by the fact that all roles need to be matured at roughly the same time and will often cut across departmental, local, national, and even regional. In this context, a city-state model like Singapore's Singpass that is a single jurisdiction and concentrated government structure, while one of the more complex is the EU's eIDAS 2.0 that spans national and regional laws and systems.

eIDAS 2.0 is often used as a model by other governments for how to develop government-issued digital credentials for their citizens, but other regions are offering leadership in this space as well. India's Aadhaar system,[20] Singapore's Singpass,[21] Italy's Public Digital Identity Systems, and various U.S. states' mobile driver's licenses are just a few of the government-issued digital credential programs used daily by a significant portion of their populations.

There are other systems in production today. The ones in this paper were selected to show the diversity of deployments currently in use.[22]

[20] Government of India, "myAadhaar," Unique Identification Authority of India, website, https://uidai.gov.in/en/.
[21] Singpass, https://www.singpass.gov.sg/main/
[22] More information on digital identity reference deployments can be found in the Secure Identity Alliance whitepaper Giving Voice to Digital Identities Worldwide. Secure Identity Alliance. "Giving Voice to Digital Identities Worldwide - Key Insights and Experiences to Overcome Shared Challenges," March 16, 2022. https://secureidentityalliance.org/utilities/news-en/entry/giving-voice-to-digital-identities-worldwide-1-1.

3.2.1 India's Aadhaar System

The largest government-issued identity program in the world when it comes to the number of registered participants and monthly transactions is India's Aadhaar system.[23] Originally launched in 2010 and significantly revised as a result of India's Supreme Court judgment in 2018, the Aadhaar system is an interesting model to consider for large-scale deployments.[24]

The body of research and reporting on the Aadhaar system post the 2018 Supreme Court judgment that found the Aadhaar system largely in compliance with India's constitution.[25] The judgement was significant in that it paved the way for Aadhaar to move into broad adoption. It included several common themes regarding the privacy considerations of the system, finding the revised system in compliance with India's constitution. India's Supreme Court aside, academic researchers and other members of civil society consider the Aadhaar system a concerning example of government surveillance of its citizens and registered residents.[26] Countering that, the government has reported that the Aadhaar system has saved the state over Rs 2 trillion (USD$24billion) over the last nine years to eliminate duplicate and fraudulent identities.[27] Obviously, this is not a like-to-like comparison, as putting a monetary value to privacy is challenging in the best of times, but it does explain the tension between moving to a national identity system and enacting strong privacy protections for individuals.

Services available to Aadhaar holders and service providers include:[28]

[23] Unique Identification Authority of India | Government of India. "Home - Unique Identification Authority of India | Government of India." Accessed April 1, 2023. https://uidai.gov.in/en/.

[24] "Justice K.S. Puttaswamy (Retd.) And Another Versus Union Of India And Others." The Supreme Court Of India, Civil Original Jurisdiction, September 26, 2018. https://uidai.gov.in/images/news/Judgement_26-Sep-2018.pdf.

[25] Supreme Court Observer. "Constitutionality of Aadhaar Act - Supreme Court Observer," December 24, 2021. https://www.scobserver.in/cases/puttaswamy-v-union-of-india-constitutionality-of-aadhaar-act-case-background/.

[26] See for example Henne, Kathryn. "Surveillance in the Name of Governance: Aadhaar as a Fix for Leaking Systems in India." Information, Technology and Control in a Changing World, June 22, 2019, 223–45. https://doi.org/10.1007/978-3-030-14540-8_11, Bhandari, Vrinda, and Karan Lahiri. "The surveillance state, privacy and criminal investigation in India: Possible futures in a post-Puttaswamy world." U. Oxford Hum. Rts. Hub J. (2020): 15, and Tyagi, Amit Kumar, Gillala Rekha, and N. Sreenath. "Is Your Privacy Safe with Aadhaar?: An Open Discussion." Grid Computing, December 1, 2018. https://doi.org/10.1109/pdgc.2018.8745836.

[27] Zee News. "Aadhaar a '"bedrock"' for Govt Welfare Schemes, Saved over Rs 2 Lakh Crore: NITI Aayog." Microsoft Start, June 1, 2022. https://www.msn.com/en-in/money/news/aadhaar-a-bedrock-for-govt-welfare-schemes-saved-over-rs-2-lakh-crore-niti-aayog/ar-AAXZ6YM

[28] Unique Identification Authority of India. "myAadhaar One portal for all online services," website, https://www.uidai.gov.in/en/16-english-uk/aapka-aadhaar/1035-view-all-services.html.

- **Verify Aadhaar Number:** This will enable service providers and Aadhaar number holders to verify if the Aadhaar number is valid and is not deactivated.
- **Verify Email/Mobile Number:** Aadhaar number holder's registered mobile number is essential to access Aadhaar online services as well as Aadhaar enabled benefits. Residents can verify their already registered email address and mobile number.
- **Lock/Unlock Biometrics:** Aadhaar number holders can secure their biometric authentication by locking their biometrics. Once locked, same cannot be used by anyone for authentication. Residents can unlock their biometrics before any biometric authentication transaction.
- **Check Aadhaar & Bank Account Linking Status:** Aadhaar holders can check if their Aadhaar is linked to their bank account. Aadhaar Linking status is fetched from NPCI Server. Under any circumstance, UIDAI shall not be responsible or liable for the correctness of the displayed status. Further, UIDAI is not storing any information fetched from NPCI server.
- **Aadhaar Authentication History:** Aadhaar number holders can view the details of Aadhaar Authentication hey have done.
- **Offline Aadhaar Data Verification:** It is a secure sharable document which can be used by any Aadhaar number holder for offline verification of Identification.
- **Virtual ID Generator:** Aadhaar Number holders can generate their 16 Digit Virtual ID(VID).

The system fundamentally depends on an individual's biometric information, which we discuss in more depth later in this paper in section 4.2.2 Biometric Technologies. Starting at age 5, even children must submit their biometric information in order to be enrolled in the system. The system also enables a new kind of surveillance, as noted by Silvia Masiero and S. Shakti:

> *"This changes the architecture of surveillance, moving it from centralized to distributed. Thus, any entity with access to such data, both public (such as providers of social protection schemes—see Nayak, this Special Issue) or private, can possess surveillance power. Moreover, as Shakthi (this Special Issue) highlights, platform owners, and by extension, the tools for surveillance, have themselves become distributed into the private sphere. This leads to a*

conception of a new type of surveillance, based on both access to, and ownership of, critical data." – Frank Hersey, Biometric Update[29]

Regardless of any privacy-related concerns, Aadhaar is considered a model deployment by many countries, resulting in an effort to create an "Aadhaar in a box" - the Modular Open-Source Identification Platform (MOSIP).[30] MOSIP is a free, open-source system gaining traction in Africa. Both the strengths and weaknesses of the Aadhaar system, including all associated privacy considerations, are likely to proliferate as countries choose this as the model for the government-issued digital credentials and identity services.

3.2.2 Singapore's Singpass

Singapore's digital identity system is called Singpass.[31] This system includes 700 organizations offering over 2000 services to 4.5 million registered users.[32] The system is heavily reliant on the Singpass mobile application, with 85% of transactions going through that interface. Services offered by Singpass include:

- 'Myinfo,' which supports pre-fill for digital forms for online transactions and serves as the source of truth for all other Singpass services.
- 'Verify' for biometric-based identity verification that enables residents to perform secure in-person identity verification and data sharing through scanning QR codes.
- 'Face Verification' is a basic authentication service that compares facial biometrics to government-held data, and 'Sign' to digitally sign documents.

In the findings from a case study conducted by the World Bank and Singapore's Government Technology Agency, 97% of the eligible population use Singpass to access

[29] Masiero, Silvia, and S. Shakthi. "Grappling with Aadhaar: Biometrics, Social Identity and the Indian State." South Asia Multidisciplinary Academic Journal, no. 23 (September 15, 2020). https://doi.org/10.4000/samaj.6279.

[30] Hersey, Frank. "Maturing MOSIP Enjoys ID4Africa Limelight as It Expands Its Partnerships and Vendors Flock." Biometric Update, March 23, 2023. Accessed April 1, 2023. https://www.biometricupdate.com/202206/maturing-mosip-enjoys-id4africa-limelight-as-it-expands-its-partnerships-and-vendors-flock.

[31] Government of Singapore. "Singpass - Your Improved Digital ID." Accessed April 1, 2023. https://www.singpass.gov.sg/main/.

[32] Government of Singapore, Smart Nation and Digital Government Office (SNDGO). "Singpass Singapore's National Digital Identity (Factsheet)." Accessed April 1, 2023. https://www.smartnation.gov.sg/media-hub/press-releases/singpass-factsheet-02032022.

online services.[33] Organizations that use the Myinfo service within Singpass report "an average decrease of up to 80 percent in application time for users, with businesses reporting up to a 15 percent higher approval rate, due to better data quality and significant cost savings in their customer acquisition process."[34] Services have confidence that the users are who they say they are, and the users enjoy the convenience of timely access to services.

Very few reports exist regarding breaches of the Singpass ecosystem. While the government is considering developing a decentralized service in the form of a Decentralized Identifier (DID) Verifiable Credential-based identity wallet, much of the system is still in centralized databases.[35] Still, privacy advocates remain concerned regarding the potential for misuse of critical personal data such as biometrics. The concern that government agencies can access biometric data for uses outside the original scope is well founded as such behavior is allowed by Singapore's Public Sector (Governance) Act (covered in more detail later in this paper). The concerns about surveillance and unconsented use of personal data between government agencies is a common theme for all government-issued digital credentials. As decentralized models emerge, it will be interesting to observe if countries like Singapore will migrate to them in an attempt to address privacy concerns, lower the transaction load on government systems, and enable more cross border usage by Singaporean citizens, residents, and businesses.

3.2.3 Italy's Public Digital Identity System

In Italy, the government has been working on government-issued digital credentials for nearly ten years. This effort is part of a larger digital transformation effort for the country. The first public system designed around the citizen and public administration was the Sistema Pubblico di Identità Digitale (SPID) or Public Digital Identity System. This system

[33] The World Bank, International Bank for Reconstruction and Development. "National Digital Identity and Government Data Sharing in Singapore: A Case Study of Singpass and APEX," 2022. pp. xiv. https://www.developer.tech.gov.sg/assets/files/GovTech%20World%20Bank%20NDI%20APEX%20report.pdf.

[34] The World Bank, International Bank for Reconstruction and Development. "National Digital Identity and Government Data Sharing in Singapore: A Case Study of Singpass and APEX," 2022. pp. 46. https://www.developer.tech.gov.sg/assets/files/GovTech%20World%20Bank%20NDI%20APEX%20report.pdf.

[35] Hersey, Frank. "Singpass Incorporates Digital Identity Card, Saves $36 per Onboarding, Considers Decentralization." Biometric Update |, September 9, 2022. Accessed April 1, 2023. https://www.biometricupdate.com/202207/singpass-incorporates-digital-identity-card-saves-36-per-onboarding-considers-decentralization.

was established in October 2014 and made operational in 2016[36], period during which also the electronic identity card (CIE) activates its digital identity system, using the same technology used by SPID. Both SPID and CIE are digital identity tools also recognized in Europe, in accordance with the eIDAS Regulation (Regulation (EU) No. 910/2014). Based on the Security Assertion Markup Language version 2 (SAML2), both SPID and CIE enable citizens to use a government-verified identity for both public and private services. The system continues to evolve as new protocols offer new functionality, and a second system based on OpenID Connect (OIDC) is being tested and is expected to move into full production in mid-2023. The new system is reviewed regularly to make sure it complies with all relevant EU regulations.

From a privacy perspective, the organizations managing these services, the Agency for Digital Italy (AGID) for SPID and the Ministry of Interiors for CIE, reviews all services requesting to use the credentials in this system, with an administrative and technical activation procedure which evaluates both administrative and technical and security requirements. Services must comply with all privacy laws; they only receive proofs of requested data and never the credential itself, and that only with the explicit consent of the individual.

While a model system within the EU, just over half of the adult population has one of these digital credentials.[37]

3.2.4 eIDAS 2.0 (electronic IDentification, Authentication, and trust Services)

The eIDAS regulation was originally established in EU Regulation 910/2014 on 23 July 2014 and has received new attention thanks to a recent revision, commonly referred to as eIDAS 2.0. Expected to be in force by September 2023, eIDAS 2.0 requires all EU member states make Digital Identity Wallets (the EUDI Wallet) available to all EU citizens, residents, and businesses that are interoperable across the EU. So, while eIDAS 2.0 is a legal construct that focuses on wallets in general and not on credentials, we have placed it in this section

[36] Agenzia per L'Italia Digitale. "SPID - Public Digital Identity System|Agenzia per l'Italia Digitale." Accessed April 1, 2023. https://www.agid.gov.it/en/platforms/spid.

[37] Mascellino, Alessandro. "Italian National Digital ID Scheme Reaches 30 Million Users Milestone." Biometric Update, May 9, 2022. https://www.biometricupdate.com/202205/italian-national-digital-id-scheme-reaches-30-million-users-milestone.

on credentials because of the future intent for those wallets to include government-issued digital credentials.

The EU is making powerful moves towards enabling digital credentials to be not just replacements for, but improvements to physical credentials. By clearly defining the architecture[38] and encouraging large-scale pilots[39], member states are seeing innovation happening rapidly and at scale. With the GDPR providing the core legal framework for the privacy protection of personal data and NIS2 establishing cybersecurity requirements that, while not specific to privacy, will enhance the privacy posture of the EU, privacy protections are a strong consideration for this new digital ecosystem.

eIDAS 2.0 requires several characteristics that enhance the privacy protection available with the use of digital credentials, most critically enabling "people to choose which aspects of their identity, data and certificates they share with third parties, and to keep track of such sharing. User control ensures that only information that needs to be shared will be shared."[40] Each member state is free to develop the technologies appropriate to eIDAS requirements; as long as the technologies interoperate across borders, the details are left to the implementers.

That said, several privacy advocates and civil societies have indicated significant concerns regarding eIDAS 2.0, ranging from issues regarding unique and persistent identifiers (enabling individual tracking and profiling) to centralization of data (raising the specter of the surveillance state).[41] In addition, the lack of legal mechanisms to identify and address criminal or fraudulent uses of the system in cross-border cases raises red flags.[42] It is also worth noting that while offering control to individuals is a necessary component to enabling privacy, it is not sufficient in that services may request more information than

[38] European Commission. "The European Digital Identity Wallet Architecture and Reference Framework." Shaping Europe's Digital Future, February 10, 2023. https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework.

[39] European Commission. "Funding & Tenders: Single Electronic Data Interchange Area (SEDIA)," December 16, 2022. https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/digital-2022-deploy-02-electronic-id.

[40] European Commission. "Commission Proposes a Trusted and Secure Digital Identity for All Europeans." Press Corner, June 3, 2021. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2663.

[41] Hoepman, Jaap-Henk. "Analysing the Architecture of the European Digital Identity Framework.," February 14, 2023. https://blog.xot.nl/2023/02/14/analysing-the-architecture-of-the-european-digital-identity-framework/index.html.

[42] epicenter.works. "EIDAS 2.0 – Unprecedented Risk for Privacy," December 1, 2022. https://en.epicenter.works/content/eidas-20-unprecedented-risk-for-privacy.

they absolutely need (though they may have a different interpretation over that need). Expecting the individual to understand all the choices open to them during a transaction where their primary goal is to get to the end result is less than ideal.

eIDAS 2.0 focuses on the wallet itself rather than defining the credential format for the credentials that governments may store in it. Guidance on the format, privacy protections, and general use of government-issued digital credentials is expected to be part of the implementation act for eIDAS 2.0.[43]

3.2.5 U.S. State Implementations

The U.S. federal government does not issue digital credentials at this time, nor are there federal-level general privacy laws.[44] That said, states within the country have started issuing government-issued digital credentials in the form of mobile driver's licenses (mDLs). Given the lack of a national identity card (i.e., national IDs) in the U.S., driver's licenses are used in many of the same ways national IDs are used in other countries.

The diversity of state-level mDL implementations–ranging from 'no implementation' to 'in production today'–makes examining the U.S. environment particularly complicated. For this paper, we look to three examples that reflect some of the diversity of the landscape: Maryland, which piloted its efforts on Apple wallets and later expanded to include Google; Arizona, which was the first state to see their mDLs accepted by the U.S. Transportation Security Administration (TA); and Utah, which went live with a standards-compliant app built for their state. In all states reviewed for the paper, the use case for mDLs is for it to be used wherever a physical license may be used. If any organization is supporting the use of these credentials in any online transactions, they have not publicized that information.

Guiding implementations in the U.S. and Canada is an organization called the American Association of Motor Vehicle Administrators (AAMVA).[45] Through the work of their AAMVA's Joint mDL Subcommittee (consisting of their Card Design Standard Subcommittee and

[43] For more information on how implementation acts are developed, see https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vha0t8afc0ya.

[44] Note that digital credential issuance by the U.S. government is in progress. See U.S. Department of Homeland Security Science and Technology Directorate. "News Release: DHS Awards $181K to Verify Digital Credentials | Homeland Security," November 14, 2019. https://www.dhs.gov/science-and-technology/news/2019/11/14/news-release-dhs-awards-181k-verify-digital-credentials.

[45] AAMVA. "Home - American Association of Motor Vehicle Administrators - AAMVA," Accessed April 1, 2023. https://www.aamva.org/.

Electronic Identity Subcommittee), AAMVA has created implementation guidelines that are critical for the interoperability of mDLs in the region.[46]

Unfortunately, but perhaps not unsurprisingly, criminals are already finding ways to commit fraud with these new credentials.[47]

3.2.5.1 Maryland

Maryland rolled out mDLs to smartphone users in 2022.[48] The credentials are created by taking a photo of the front and back of their physical driver's license and a short video of themselves, which is then sent to issuing authorities for verification. When the information is verified, the individual may add it to their Google or Apple wallets and, where accepted, use it in place of the physical credential. This is a common pattern with other states as well.

Maryland is also one of the states that has a law focused on privacy: the Personal Information Protection Act (PIPA).[49] This law, however, is focused on consumer use cases and does not explicitly support the use of mDLs. Instead, the Maryland Department of Transportation's Motor Vehicle Authority (MDOT MVA) includes a Terms and Conditions agreement for mDL holders. This describes how and when information will be shared between the Digital Wallet provider and the MDOT MVA. However, it also includes the disclaimer that the "MDOT MVA does not control the privacy and security of your information that may be held by the Digital Wallet provider and that is governed by the privacy policy given to you by the Digital Wallet provider."[50]

3.2.5.2 Arizona

Arizona went live in early 2022 with the first Apple wallet mDL implementation. Holders of these mDLs were able to use these new credentials anywhere a physical driver's license

[46] American Association of Motor Vehicle Administrators - AAMVA. "Mobile Driver License." Accessed April 1, 2023. https://www.aamva.org/topics/mobile-driver-license#?wst=4a3b89462cc2cff2cbe0c7accde57421.

[47] McConvey, Joel R. "Banks Hit with Biometric Fraud, Fake Mobile Driver's Licenses." Biometric Update, March 20, 2023. https://www.biometricupdate.com/202303/banks-hit-with-biometric-fraud-fake-mobile-drivers-licenses.

[48] Pascale, Jordan. "Maryland Launches Digital Version Of Driver's License On IPhone." DCist, May 26, 2022. https://dcist.com/story/22/05/26/maryland-digital-drivers-license/.

[49] Maryland General Assembly. "The Personal Information Protection Act (PIPA), Md. Code Ann. Comm. Law 14-3504," April 30, 2019. http://mgaleg.maryland.gov/mgawebsite/Laws/StatuteText?article=gcl§ion=14-3504&enactments=False&archived=False.

[50] Maryland Department of Transportation Motor Vehicle Administration. "Mobile Driver's License (MDL) Terms and Conditions," April 12, 2022. https://mva.maryland.gov/Documents/mDL-Terms-and-Conditions.pdf.

would be used. In addition, these credentials could be used at designated TSA airport security checkpoints in Phoenix Sky Harbor International Airport, an important tie to federal systems.[51]

Arizona is not one of the U.S. states with a digital privacy law. Instead, they rely on a generic privacy policy statement on their website.[52] For the mDL release, the privacy considerations were largely in the hands of Apple, which maintains control of the marketing, rollout, and device support for the program. This has raised concerns with privacy advocates, but those concerns have not been reflected in any new legislation at this time.[53]

3.2.5.3 Utah

Utah was arguably the first state in the U.S. to issue mDLs. Rather than partner with Google or Apple, they choose to engage with a third party for their implementation, GET Group North America and the mobile digital ID vendor Scytáles.[54] The path to implementation was not, however, entirely smooth. Discussions in 2021 of an amendment (S.B. 88) to the original bill legislating mobile driver's licenses in the state served as a lightning rod to individuals fearful of the technology and its implications in their lives.[55] The result of that debate–dropping the proposed amendment–actually negated several additional privacy protections being proposed, including text such as:

> *(4) The division shall ensure that the system and technology used for an electronic license certificate or identification card*
>
> *(i) maintains the data security and privacy of the individual in the same manner as an individual with a license certificate or an identification card*

[51] Arizona Department of Transportation. "Arizonans Are First in the Nation to Add Driver Licenses to Apple Wallet | ADOT," March 23, 2022. https://azdot.gov/adot-news/arizonans-are-first-nation-add-driver-licenses-apple-wallet.

[52] State of Arizona. "Privacy Policy." Accessed April 1, 2023. https://az.gov/policy/privacy.

[53] MacDonald-Evoy, Jerod. "Apple Digital Driver's License in Arizona Raise Privacy Concerns." AZ Mirror, March 25, 2022. https://www.azmirror.com/2022/03/25/apple-digital-drivers-license-in-arizona-raise-privacy-concerns/.

[54] Nash, Jim. "Mobile Driving Licenses Live in Utah, Arizona for Credit Union Transactions." Biometric Update, August 11, 2022. https://www.biometricupdate.com/202208/mobile-driving-licenses-live-in-utah-arizona-for-credit-union-transactions.

[55] Beal-Cvetko, Bridger. "Is Misinformation about COVID, United Nations a Trend at Utah Capitol?" Deseret News, March 11, 2022. https://www.deseret.com/utah/2022/2/8/22923842/misinformation-conspiracy-theories-utah-legislature-united-nations-salt-lake-city-digital-ids.

(ii) is not capable of digital tracking, geotracking, or other data collection from the device or the end user[56]

Whether new legislation will be introduced is uncertain. The situation for Utah, as well as for the rest of the U.S., is moving rapidly.

[56] Utah State Legislature. "S.B. 88 Digital Driver License Amendments," March 4, 2022. https://le.utah.gov/~2022/bills/static/SB0088.html.

596

597 ### 3.2.6 Summary

598

ID System	Number of identities	Services Supported	Usable by third-parties	Reported identities impacted by security breaches	Privacy considerations
Aadhaar	**1.359 billion (~88% of total population)**	welfare payments and social services; cashless payments (see the Universal Payment Interface)	Yes	over 1 billion records exposed in a single breach in 2018.[57]	India's Supreme Court noted the following:[58] • The Unique Identification Authority of India (UIDAI) does not collect purpose, location, or details of transactions. • What information is being collected reasonably balances the right to privacy and the right to basic human services such as food, shelter, and employment. • An Aadhaar identifier cannot be required to open a bank account (thought it can be required for certain government services).

[57] World Economic Forum. "The Global Risks Report 2019," January 15, 2019. https://www.weforum.org/reports/the-global-risks-report-2019/.

[58] Doshi, Menaka. "Aadhaar: A Quick Summary Of The Supreme Court Majority Order." BQ Prime, September 27, 2018. https://www.bqprime.com/aadhaar/aadhaar-a-quick-summary-of-the-supreme-court-majority-order.

Singpass	**4.2 million (97% of eligible residents)**	2,000 services by over 700 government agencies and businesses	Yes	1500	- Singpass facial verification technology only collects the data that is needed for a specific purpose - photo for facial recognition is retained on government servers for 30 days - only a matching score when the facial image is verified against the government biometric database is shared with third-parties (i.e., private sector)
SPID	**33 million (63% adult population)**	Over 12,000 public administrations are offering at least one service online through SPID by November 2022. 141 private companies had joined SPID by October 2022.[59]	Yes	n/a	This service must comply with all applicable EU and national laws and regulations (e.g., GDPR, NIS2, eIDAS2.0)
eIDAS	**447 million (TBD)**	under development; use cases informing eIDAS include: general online services,	Yes	n/a	

[59] Tosques, Lara. "State of Play on Adoption of Digital Identity in Italy 2022." Namirial.Com, December 1, 2022. https://www.namirial.com/en/news/digital-identity-state-of-play-italy-end-of-2022/.

		mobility and digital driving license, health, educational credentials and professional qualifications, digital finance, and digital travel credentials[60]			
U.S. stats	unknown	mobile driver's licenses	Yes	n/a	Each state is approaching privacy differently; there is no consistent pattern at this time in the U.S.

3.3 Technological Diversity and Capability

With regulation providing one level of protection for how governments and other entities may issue digital credentials and subsequently use that data, technology offers its own threats and opportunities for supporting the privacy of individuals and security for government-issued and managed data. One of the biggest challenges with technology is the consideration that technology itself is neutral; whether it is "good" or "bad" depends on how it is being used. Biometrics, for example, may enable secure and easy access to systems and services; it can also enable unethical tracking. Basic logging of transactions supports the security and accountability of a system; it can also be used to correlate a user's activities on the web. And perhaps most critically, requiring consent allows the individual to make their own decisions; it is also often ignored by the individual in favor of immediate gratification.[61] What is reasonable and appropriate in one situation may be harmful and unnecessary in another; technology cannot make that judgment call. Attempts to bridge that gap with consent banners results in a user experience that drives individuals to ignore the messages.

[60] "The European Digital Identity Wallet Architecture and Reference Framework." https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework.
[61] Solove, Daniel. "Murky Consent: An Approach to the Fictions of Consent in Privacy Law." TeachPrivacy, January 23, 2023. https://teachprivacy.com/murky-consent-an-approach-to-the-fictions-of-consent-in-privacy-law/.

Still, there may be more that technology can do to help bridge the gap between trusting regulatory control and building in privacy protections at the lowest layer possible. Governments rely on technology to support the promise of digital transformation while simultaneously protecting their people, so considering what it can and cannot do is critical to understanding the full scale of what's possible and where more work is needed.

Privacy Considerations for Internet Protocols (RFC 6973)

In 2013, the Internet Engineering Task Force (IETF), the home of so many Internet standards and best practices, developed guidance on when and how to write a privacy considerations section for any RFC where user privacy is potentially impacted. Ultimately, this RFC "aims to make designers, implementers, and users of Internet protocols aware of privacy-related design choices."

Since its publication, 101 RFCs (out of nearly 2500 published since RFC 6973) have included an explicit privacy considerations section. In addition, seven RFCs (one being an update of another in that list) are exclusively about the privacy considerations for a specific protocol (see "DNS Privacy Considerations" (RFCs 7626 and 9076), "Security and Privacy Considerations for IPv6 Address Generation Mechanisms" (RFC 7721), "Privacy Considerations for DHCP" (RFC 7819), "Privacy Considerations for DHCPv6" (RFC 7824), "Privacy Considerations for IPv6 Adaptation-Layer Mechanisms" (RFC 8065), and "Privacy Considerations for Protocols Relying on IP Broadcast or Multicast" (RFC 8386).

Standardized guidance of this type is a useful component to encourage specification authors to think more broadly about the technology they are defining. This guidance has been used by other standards organizations as well, including the OpenID Foundation and OASIS. It is not, however, required or consistently used, nor are the specification authors always the best individuals to understand and document the privacy implications of their specifications.

3.3.1 The Technology Behind Digital Credentials

Enabling and enhancing individual privacy as part of the issuance and use of government-issued digital credentials requires laws and technology to work together. This section reviews the most common technologies either in use or under consideration for these credentials today.

3.3.1.1 Digital Wallets

At its most simple, a digital wallet is an application on a device that stores digital credentials. Individuals with smartphones are becoming familiar with them as they store transit cards, airline boarding passes, loyalty cards, and more. The requirements for identity wallets, however, are more robust than for the other use cases. Identity wallets are intended to help an individual select what personal data they wish to present to the requesting service, including their consent for the transaction using whatever protocol the service and wallet jointly support. Since wallets aim at hosting various credentials and address multiple use cases, the need to support multiple formats of credentials is increasing, along with the need to present your attributes in a connected or unconnected manner.

The exact details of how digital identity wallets secured are not specified in any standard at the time of publication for this paper. However the ISO comity is working on the ISO 23220 series which intends to define some foundational on issuance, trust, and provisioning. Standardization of wallets is implied by the need for the wallet to support common patterns such as issuance and presentation for the credentials they contain.

Wallet development is happening in both the public and private sectors. As mentioned earlier in this paper, eIDAS 2.0 is bringing the reality of a European Digital Identity Wallet to all member states with the first pilots in 2023/2024. To address all needs, the EU regulators are designing the EU Digital ID Wallet to support multiple formats of credentials which will be based on different standards to support a wide range of use cases.

The Open Wallet Foundation, announced by the Linux Foundation in September 2022 and launched in February 2023, is focused on "best practices for digital wallet technology through collaboration on standards-based OSS components that issuers, wallet providers and relying parties can use to bootstrap implementations that preserve user choice, security and privacy."[62]

3.3.1.2 SAML2

The Security Assertion Markup Language (SAML) standard, initially published by OASIS in 2001 and a major revision (SAML2) published in 2005, is a standard for transferring authentication and authorization data between an identity provider (IdP) and a service

[62] "OpenWallet Foundation – Linux Foundation Project." Accessed April 1, 2023. https://openwallet.foundation/.

provider (SP).[63] This protocol was designed to achieve cross-domain single sign-on (SSO) in a browser. SAML2 is still in widespread use today in several sectors including education and government. Active development, however, ceased around 2012.

From the SAML 2.0 specification:

> *4.5 Privacy in SAML*
>
> *In an information technology context, privacy generally refers to both a user's ability to control how their identity data is shared and used, and to mechanisms that inhibit their actions at multiple service providers from being inappropriately correlated.*
>
> *SAML is often deployed in scenarios where such privacy requirements must be accounted for (as it is also often deployed in scenarios where such privacy need not be explicitly addressed, the assumption being that appropriate protections are enabled through other means and/or layers).*
>
> *SAML has a number of mechanisms that support deployment in privacy.*
>
> - *SAML supports the establishment of pseudonyms established between an identity provider and a service provider. Such pseudonyms do not themselves enable inappropriate correlation between service providers (as would be possible if the identity provider asserted the same identifier for a user to every service provider, a so-called global identifier)*
> - *SAML supports one-time or transient identifiers – such identifiers ensure that every time a certain user accesses a given service provider through a single sign-on operation from an identity provider, that service provider will be unable to recognize them as the same individual as might have previously visited (based solely on the identifier, correlation may be possible through non-SAML handles).*
> - *SAML's Authentication Context mechanisms allow a user to be authenticated at a sufficient (but not more than necessary) assurance*

[63] OASIS Security Services (SAML) Technical Committee. "SAML V2.0 Standard." FrontPage - SAML Wiki, June 26, 2020. https://wiki.oasis-open.org/security/FrontPage.

level, appropriate to the resource they may be attempting to access at some service provider.

- *SAML allows the claimed fact of a user consenting to certain operations (e.g. the act of federation) to be expressed between providers. How, when or where such consent is obtained is out of scope for SAML.*

While still used throughout the world, SAML2 is not without significant limitations. For example, given that SAML is expressed using the eXtensible Markup Language (XML), mobile platforms often cannot support it, as XML parsers were not built into mobile platforms. And, given that user consent must be handled entirely outside the protocol means that SAML was not a perfect fit in a mobile context. SAML2, when used carefully and in conjunction with other mechanisms (such as a consent manager) and with a full understanding of its complexity, can be used in a privacy-preserving online environment, but it is not simple.

3.3.1.3 OAuth2

The Internet Engineering Task Force (IETF) develops Internet technical standards at every layer of the network stack, from transporting bits across a network to application-level interoperability. In the realm of authentication and authorization, their standards provide direction beyond just the application layer. That said, in the digital credential space, their most influential standards for application-level authentication and authorization are in the OAuth group of documents.

While mapping the relationships of OAuth specifications is out of scope for this document, understanding how they impact government-issued digital credentials and the overall impact they have on privacy is in scope.

The OAuth 2.0 specifications define how clients, such as applications on mobile devices, secure access to the user resources on a service provider (e.g., a government agency's service portal). The delegated authorization framework and API at the core of the OAuth specifications are critical to supporting authentication and authorization on mobile devices.

"SAML was not a perfect fit in a mobile context. XML parsers were not built into mobile platforms, and cryptographic requirements were heavy. The resulting access management paradigm was OAuth 1.0, a "delegated authorization

framework" that could layer with federated protocols. OAuth addresses the 'user not present' scenario: applications ask for and receive an "access token" that does not introduce the user; instead, access tokens represent the ability to access a tightly scoped set data and services on behalf of a user." – Pamela Dingle, Introduction to Identity - Part 2: Access Management[64]

The specification family for OAuth 2.0 is well-developed but not static. Individuals continue to propose and standardize new features or offer improvements to existing ones via the OAuth working group within the IETF.[65]

For individuals implementing OAuth2, perhaps the biggest challenge is understanding how all the different specifications relate to each other, and which should be used in a given situation. Developers may implement only parts of the specification, missing elements such as token signatures for security or the correct use of JSON Web Tokens (JWT) for more efficient requests for user information. There are no certification mechanisms for OAuth2 compliance, and while guidance exists on the web, knowing what rules to follow is always a challenge.

While technically an authorization protocol rather than an authentication protocol, OAuth2 is tightly enough coupled to authentication that many developers confuse the scope of OAuth2 to include authentication.[66] For an actual authentication protocol, one should look to the OpenID Connect (OIDC) set of specifications.

3.3.1.4 OpenID Connect

The OIDC set of specifications is developed and maintained within the OpenID Foundation.[67] The OpenID Foundation publishes technical specifications, profiles, and white papers, as well as offering certification services to publicly verify compliant implementations.

[64] Dingle, Pamela. "Introduction to Identity - Part 2: Access Management." IDPro Body of Knowledge 1, no. 2. June 18, 2020. https://doi.org/10.55621/idpro.45.
[65] IETF. "Web Authorization Protocol (Oauth)." Accessed April 1, 2023. https://datatracker.ietf.org/wg/oauth/documents/.
[66] Richer, Justin. "End User Authentication with OAuth 2.0." Accessed April 1, 2023. https://oauth.net/articles/authentication/.
[67] "OpenID Foundation Website." OpenID Foundation homepage. Accessed April 1, 2023. https://openid.net/.

The foundational OIDC specification, OIDC Core, "defines the core OpenID Connect functionality: authentication built on top of OAuth 2.0 and the use of Claims [a piece of information asserted about an Entity] to communicate information about the End-User. It also describes the security and privacy considerations for using OpenID Connect.".[68] Work is underway within the OpenID Connect Working group to further define the use of OIDC with verifiable credentials and self-issued OpenID providers.[69] This positions the specification to support efforts around digital wallets and direct control by individuals for their own data.

Going beyond the OIDC specifications, the OpenID Foundation includes profiles that constrain the general specification for appropriate use in specific industries. From the Financial-grade API (API) for the finance industry to Health Relationship Trust (HEART) profiles for the healthcare industry, these profiles describe what aspects of OIDC are appropriate for these use cases. As with all profiles, their guidance can only limit what is in the original specification; it does not add new, conflicting requirements.

3.3.1.5 Verifiable Credentials

The concept of a verifiable credential, which at its most basic is a digital credential that can be verified in some manner, is widespread. Whether governments and organizations are specifically referring to W3C Verifiable Credentials (VCs) or some other, potentially proprietary, form of verifiable credential requires research into each implementation.

Focusing on VCs as standardized within the World Wide Web Consortium (W3C), VCs were designed with government-issued digital credentials as one of the driving use cases.[70] As per the specification's abstract, "A *verifiable claim* is a qualification, achievement, quality, or piece of information about an entity's background such as a name, government ID, payment provider, home address, or university degree."

[68] Sakimura, Nat, J. Bradley, M. Jones, B. De Medeiros, and C. Mortimore. "OpenID Connect Core 1.0 Incorporating Errata Set 1," November 8, 2014. https://openid.net/specs/openid-connect-core-1_0.html.
[69] OpenID Connect Working Group. "OpenID for Verifiable Credentials" OpenID Foundation. Accessed April 1, 2023. https://openid.net/openid4vc/.
[70] Otto, Nate, Sunny Lee, Brian Sletten, Daniel Burnett, Manu Sporny, and Ken Ebert. "Verifiable Credentials Use Cases: W3C Working Group Note 24 September 2019," September 24, 2019. https://www.w3.org/TR/vc-use-cases/.

The privacy considerations section of the core VC specification is extensive.[71] It recognizes that privacy is not a binary concept and that government-issued identifiers are often highly correlatable.

While not restricted to blockchains, countries exploring blockchain technologies have relied on VCs for their services. The European Blockchain Services Infrastructure (EBSI), an initiative of the European Commission and the European Blockchain Partnership, required support for the Verifiable Credentials Lifecycle "to understand how Verifiable Credentials work according to W3C and EBSI standard."[72]

3.3.1.6 ISO/IEC 18013-5:2021 Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application

The acceptance of driving licenses at the international level down to the most local jurisdiction makes driver's licenses one of the most influential sources of identification in the world.

Such level of interoperability is driven by standardization, and because card-based driver's licenses are already expected to follow international standards, mobile driving licences (mDLs) similarly require the same interoperability. As such, the ISO/IEC 18013 group of standards for driver's licenses was extended to include and cover mobile Driving License credentials under "ISO/IEC 18013-5 -2021 - Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application."[73]

As per the abstract for this standard:

> *This document establishes interface specifications for the implementation of a driving licence in association with a mobile device. This document specifies the interface between the mDL and mDL reader and the interface between the mDL reader and the issuing authority infrastructure. This document also enables parties other than the issuing authority (e.g. other issuing authorities, or mDL verifiers in other countries) to:*
> — *use a machine to obtain the mDL data;*
> — *tie the mDL to the mDL holder;*
> — *authenticate the origin of the mDL data;*
> — *verify the integrity of the mDL data.*
> *The following items are out of scope for this document:*

[71] Sporny, Manu, Dave Longley, and David Chadwick. "Verifiable Credentials Data Model v1.1," March 3, 2022. https://www.w3.org/TR/vc-data-model. See Section 7. Privacy Considerations

[72] European Commission European Blockchain Services Infrastructure. "Success Stories." Accessed April 1, 2023. https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Verifiable+Credentials+Success+Stories.

— *how mDL holder consent to share data is obtained;*
— *requirements on storage of mDL data and mDL private keys.*

ISO/IEC 18013-5 was designed with the core ISO/IEC privacy principles in mind (see ISO/IEC 29100:2011).[74] These principles include: consent and choice, purpose specification and data retention, data minimization, collection limitation, accuracy and quality, openness, transparency, and individual participation, accountability and privacy compliance, and information security.[75]

The move towards mDLs, therefore, has a significant potential for influencing the scope, use, and privacy expectations of any government-issued digital credentials globally.

To complement the published ISO 18013-5 that addresses in person presentation of a credential, 18013-7 will soon follow suite to cover online presentation of credentials The specification family will also contemplate provisioning standards with 18013-4 and certification standards with 18013-6. All in all, the ISO mDL standard will cover a wide range of functionalities (in person verification in both connected and non-connected mode, online verification, etc..) which will open the door to new use cases while keeping end users in control of their data.

While ISO/IEC 18013-5 is limited in scope to mDLs, the level of detail regarding the communication protocols, data encodings, security mechanisms and data privacy and minimization requirements can be applied to and benefit other types of digital credentials such as identity, health credentials, etc… in a multiple credential wallet approach.

[74] ISO/IEC 29100:201. https://www.iso.org/standard/45123.html.
[75] Kelts, David. "Successful Adoption of Mobile ID Hinges Largely on Protection of Citizen Privacy." International Association of Privacy Professionals, March 1, 2022. https://iapp.org/news/a/successful-adoption-of-mobile-id-hinges-largely-on-protection-of-citizen-privacy/.

Developing a Privacy-Enhancing Model for Mobile Credentials

The Privacy Enhancing Mobile Credentials Work Group (PEMC WG) at the Kantara Initiative is working on creating a set of privacy requirements for Issuers, Verifiers, and Providers of digital identity credentials so that each stakeholder can demonstrate their conformance to these requirements. At the heart of the PEMC WG process is to ensure that the reasonable privacy expectations of the individual holding the credential are met. The "Trust Triangle" below illustrates the key stakeholders in the ecosystem. At each intersection, the stakeholder could be an individual or organization, and different standards could apply, but the privacy requirements would be similar in this decentralized model.

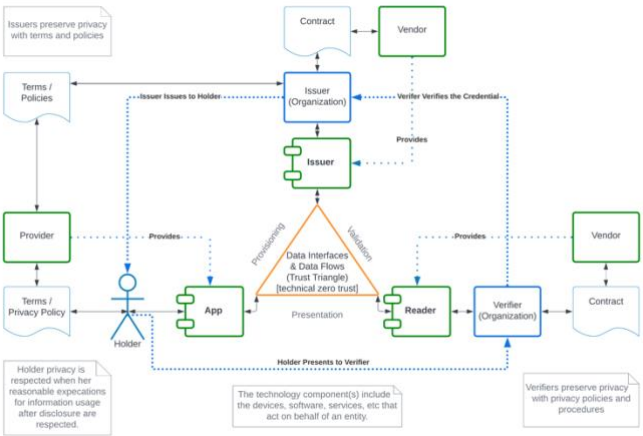


Figure 1: the PEMC Trust Triangle model

Work is currently underway for the Early Implementor's Guidance report and interested parties are encouraged to join the PEMC WG. The PEMC working group will continue to progress definition of the detailed requirements and ultimately conformance processes. This work can provide a reasonable foundation for market participants to self-certify conformance to shared privacy guidelines, a key first step.

However, this is the start of the journey. There are limits to the potential impact as there are no current policies that mandate conformance to these guidelines, nor are there mechanisms to automate conformance at scale (e.g. manual review of implementations by auditors vs automated test suites that are possible on protocols.

3.3.2 The Standards Behind Biometrics

All digital credentials described in this paper include some use of biometrics. Three of the popular sets of standards that exemplify how to use digital credentials in a privacy-preserving manner include FIDO2, NIST SP 800-63-3, and ISO/IEC 27553.[76]

3.3.2.1 Fast IDentity Online (FIDO)

The FIDO Alliance and their FIDO2 specification have significantly improved the security features available in the authentication process. Those features, including keeping biometric data on the device and under the user's control and offering unique keys for each Internet site to prevent tracking users across sites, are an example of building in privacy features at the protocol layer.[77]

3.3.2.2 NIST SP 800-63-3 Digital Identity Guidelines

NIST SP 800-63 has been a profoundly influential set of standards since its initial publication in December 2011. Since then, these guidelines have gone through two revisions and are in the process of completing a third (NIST SP 800-63-4). The purpose of these guidelines is to "provide technical guidelines to credential service providers (CSPs) for the implementation of digital authentication."[78] Government-issued digital credentials are generally issued for specific services; they are not part of any national-level identity scheme.

While the guidelines provide direction mandatory for U.S. government agencies, governments around the world have found the contents useful to their own issuance of digital credentials. NIST SP 800-63-3 took a new approach to assurance, retiring the concept of a single level of assurance and considering the different elements of risk associated with the authentication process:

> *"These guidelines provide mitigations of an authentication error's negative impacts by separating the individual elements of identity assurance into discrete, component parts. For non-federated systems, agencies will select two components, referred to as Identity Assurance Level (IAL) and Authenticator*

[76] Note that the list of interesting standards in this space is growing; this is just a sample.

[77] FIDO Alliance. "FIDO2 - FIDO Alliance." Accessed April 1, 2023. https://fidoalliance.org/fido2/.

[78] Grassi, Paul, Justin Richer, Sarah Squire, James Fenton, Ellen Nadeau, Naomi Lefkovitz, Jamie Danker, Yee-Yin Choong, Kristen Greene, and Mary Theofanos. "Digital Identity Guidelines Federation and Assertions: Federation and Assertions." National Institute of Standards and Technology, U.S. Department of Commerce, June 2017. https://doi.org/10.6028/NIST.SP.800-63c. See Section 1 Purpose.

Assurance Level (AAL). For federated systems, agencies will select a third component, Federation Assurance Level (FAL).

These guidelines retire the concept of a level of assurance (LOA) as a single ordinal that drives implementation-specific requirements. Rather, by combining appropriate business and privacy risk management side-by-side with mission need, agencies will select IAL, AAL, and FAL as distinct options. While many systems will have the same numerical level for each of IAL, AAL, and FAL, this is not a requirement and agencies should not assume they will be the same in any given system." – Paul Grassi, Michael Garcia, and James Fenton, NIST SP 800-63-3 [79]

3.3.2.3 ISO/IEC 27533

This standard, currently in two parts, provides a collection of high-level requirements for biometric authentication on mobile devices. Part 1 focuses on what the standard refers to as 'local modes,' biometric data and derived biometric data do not leave the device. In other words, the standard focuses on the protection of biometric data on the device itself, not as it relates to access to remote, off-device services. This standard was approved and published in November 2022.[80]

Part 2, still under development, picks up where Part 1 leaves off and focuses on remote modes where the biometric data "the biometric data or derived biometric data are transmitted between the mobile devices and the remote services in either or both directions."[81]

[79] Grassi, Paul, Michael Garcia, and James Fenton. "Digital Identity Guidelines." National Institute of Standards and Technology, U.S. Department of Commerce, June 2017. https://doi.org/10.6028/NIST.SP.800-63-3. See the Executive Summary.

[80] ISO/IEC 27553-1:2022 Information security, cybersecurity and privacy protection — Security and privacy requirements for authentication using biometrics on mobile devices — Part 1: Local modes. ISO/IEC JTC 1/SC 27. Geneva, Switzerland: ISO, published November 2022. https://www.iso.org/standard/71671.html.

[81] ISO/IEC WD 27553-2 Information security, cybersecurity and privacy protection — Security and privacy requirements for authentication using biometrics on mobile devices — Part 2: Remote modes. ISO/IEC JTC 1/SC 27. Under development. https://www.iso.org/standard/71670.html.

3.3.3 Identity Assurance

Perhaps the most valuable characteristic of a government-issued digital identity credential is the degree of confidence it offers that a person's claimed identity is their real identity as determined by the government. Not all use cases require the same assurances, however, which has driven a need to classify and provide guidance for how to reach various levels of identity assurance.

This section touches on a few of the standards in use today to help governments and organizations grapple with how to create the necessary assurances around an individual's digital identity.

3.3.3.1 NIST SP 800-63A

We have mentioned NIST SP 800-63-3 in general, but it is worth highlighting the specific NIST standard associated with identity assurance, NIST SP 800-63A.[82] The guidance in NIST publications is specifically targeted to U.S. federal government agencies. In its favor, the standard recognizes the need to balance organizational and government requirements, usability, and privacy. However, in attempting to address the myriad use cases that an organization the size of the U.S. government might encounter, the complexity of having multiple identity assurance levels along with different authenticator assurance levels (NIST SP 800-63B) and federation assurance levels (NIST SP 800-63C) makes compliance challenging.

3.3.3.2 Kantara Initiative Identity Assurance Framework

The Kantara Initiative's goal is to offer a technical bridge between the technology and the standards, offering an assessment program "to a range of parties who have an interest in, and reliance upon, the degree of rigor applied to the management, operation and provisioning of electronic Identity Proofing and Credential Management services."

The Identity Assurance Framework, the core of their assessment program, is strongly aligned to ISO/IEC 17065 Conformity Assessment for products and services.[83] The program

[82] Grassi, Paul, James Fenton, Naomi Lefkovitz, Jamie Danker, Yee-Yin Choong, Kristen Greene, and Mary Theofanos. "Digital Identity Guidelines: Enrollment and Identity Proofing Requirements." National Institute of Standards and Technology, U.S. Department of Commerce, June 2017. https://doi.org/10.6028/NIST.SP.800-63a.

[83] Kantara Initiative Leadership Council. "Identity Assurance Framework." Accessed April 1, 2023. https://kantara.atlassian.net/wiki/spaces/LC/pages/1737392/Identity+Assurance+Framework.

is used by U.S. government agencies to help make purchasing decisions from companies and providers certified to be in compliance with NIST SP 800-63-3.

3.3.3.3 OpenID Connect for Identity Assurance 1.0

Looking to a more code-driven specification, the OpenID Foundation published the OpenID Connect for Identity Assurance standard in 2022.[84] This specification provides an extension to OIDC that allows a service to identity information along with an explicit statement about the verification status of that information, such as what framework the information was verified under and using what evidence was used at the time of verification.

This specification is in use by several national digital identity programs being developed as part of eIDAS 2.0.[85]

3.3.4 Open Standard Identity APIs (OSIA)

In order for the technology to work together in all the ways necessary for a supportable, functional system, it needs to exist in coherent framework. This is where OSIA comes in.[86]

In 2019 multiple organizations committed to the development of national identification systems that are inclusive, trusted, and accountable and supported the development of a set of shared 'Principles for Good Identification'.[87]

The vision was to create a guiding framework that governments around the globe can use to ensure they build inclusive and trusted digital ID and civil registration systems that both enhance people's lives – and empower them to gain access to social and economic opportunities.

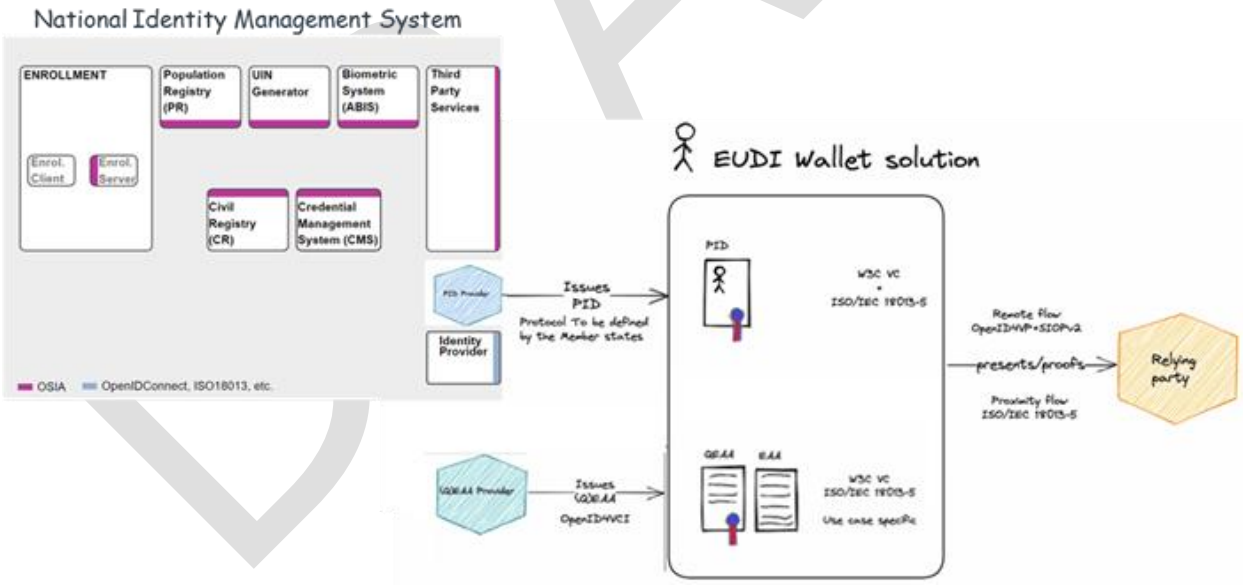
Principle 5, "[u]sing open standards and ensuring vendor and technology neutrality," enshrines the importance of enabling ID systems that utilize open standards to both

[84] Lodderstedt, Torsten, D. Fett, M. Haine, K. Lehmann, A. Pulido, and K. Koiwai. "OpenID Connect for Identity Assurance 1.0," August 19, 2022. https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html.
[85] Sharif, Amir, Matteo Ranzi, Roberto Carbone, Giada Sciarretta, Francesco Antonio Marino, and Silvio Ranise. "The EIDAS Regulation: A Survey of Technological Trends for European Electronic Identity Schemes." Applied Sciences 12, no. 24 (December 10, 2022): 12679. https://doi.org/10.3390/app122412679.
[86] Secure Identity Alliance. "OSIA." Accessed April 4, 2023. https://secureidentityalliance.org/osia.
[87] The World Bank, ID4D. "1. PRINCIPLES | Identification for Development." Accessed April 4, 2023. https://id4d.worldbank.org/guide/1-principles.

achieve improved efficiencies and functionality and assure that ID systems can be evolved and adapted to accommodate changes over time. OSIA provides the open standard interfaces (APIs) that enable seamless connectivity between building blocks of the ID management system – regardless of technology, solution, architecture, or vendor. The ITU-T has qualified this standard so that it may be normatively referenced in ITU-T standards.[88]

A government-issued digital credential, be it a driving license, an ID card or a passport, is only the tip of the iceberg of the complex set of building blocks necessary to safely issue the credential to the citizen's wallet.

All those building blocks handle the collection of personal data from the citizens, biographic and/or biometrics, its treatment to ensure identity unicity and potentially its storage. Below is a standardized view of the national identification systems building blocks from OSIA standard.[89]



As per eIDAS 2.0, National Identification Systems represent the root of trust from which the PID can be derived and issued to digital ID wallets. While today there is no selected

[88] Secure Identity Alliance. "Secure Identity Alliance Awarded Qualified ITU-T Reference Organization Status - Landmark Qualification Enables the ITU-T to Normatively Reference OSIA Specifications," November 11, 2022. https://secureidentityalliance.org/news-events/news/secure-identity-alliance-awarded-qualified-itu-t-reference-organization-status.

[89] Secure Identity Alliance. "2. Functional View — OSIA 6.2.0-DRAFT Documentation." Accessed April 4, 2023. https://osia.readthedocs.io/en/latest/02%20-%20functional.html.

standard for the PID issuance protocol, OSIA standard can help the PID provider to tap into relevant databases and systems to collect the PID and proceed with the issuance.

Already implemented in several countries, OSIA scope is as follow:

1. Build a common understanding of the functional scope for building blocks of the national identity management system

OSIA's first step has been to formalize the definitions, scope, and main functionalities of each building block within the identity management system.

2. Create a set of standardized interfaces

For this core piece of work, OSIA is focused on developing the set of interfaces needed to connect the multiple identity system building blocks and ensure seamless interactions via pre-defined services.

4 Gaps and Risks

Even working from positive intentions, regulations and technologies struggle to manage the risks to privacy that come from the integration of digital and real-world identities. In the case of regulation, the challenge comes from trying to find a balance between competing operational requirements, human nature, and technological limitations. In the technical standards community, specifying in the technology what are essentially moral and ethical choices is nearly impossible without resorting to significant bias towards one culture or another. Complicating matters are individual expectations when it comes to when and how they are expected to use their credentials.

There is room for improvement on both sides, but it requires awareness on both sides on how to leverage the strengths of each party to cover the limitations inherent in their areas of control.

This section examines some of the gaps introduced by competing motivations and the limits of what technology and regulation can realistically do to support privacy when using government-issued digital credentials.

4.1 Recognizing Motivations at Scale

When considering government-issued digital credentials on a global scale, we must recognize that while the desire for digital transformation is the same, the impetus driving those desires are quite different. This leads to a different weight being placed on each factor as they are considered before establishing a service.

Developing countries see digital identity and strong levels of identity assurance as a necessary enabler allowing people to engage in economic opportunities. In more robust economies, digital identity is more of a convenience; the depth and breadth of citizen-supporting infrastructure has been sufficient enough to stand on its own without major technological enhancements (though of course some improvements have been required to move forward). The belief of digital identity as solely an enabler of economic opportunity or a convenience in a modern world is changing; the change is being driven by a world where the lines between “online” and “offline” are blurring thanks to the ubiquity of mobile devices.

The fact that the motivations are varied is important because any effort to address the risks and gaps in the system will also vary in response to what is driving the effort. If the primary driver is financial, for example, then addressing the privacy risk must be framed as an economic benefit. If the primary driver is convenience, then the expectations of the individual users drive the experience and the demand. And in all cases, the requirements of regulation and the capability of technology frame the possible.

4.1.1 Hyper-local Expectations

The motivations driving governments are often considered at the scale of entire countries or regions. That said, there are also relevant motivations driving the parties consuming these credentials and the individuals using them. Businesses, organizations, and even individuals must consider the benefits of using high-value, government-validated information against the risks of this information being used in unexpected, unintended, and possibly inappropriate ways.

"Inherent in the capture, storage, and use of sensitive personal data are risks associated with privacy violations, data theft and misuse, identity fraud, and discrimination." – The World Bank Identification For Development Program[90]

When every entity involved in a transaction using a government-issued digital credential has a responsibility for an individual's privacy, they all bring their own expectations and requirements into the user experience. This often results a privacy paradox between individuals' stated privacy preferences and their actual disclosure behavior.[91]

4.2 The Limits of Technology

Government-issued digital credentials rely on various technology standards and tools, but the field of adoption is both wide, with multiple protocols being implemented, and narrow, in that there are only a few mobile platforms on which these tools can be used. In many cases, the technical standards are open to a variety of implementations that may result in more confusion rather than greater interoperability.[92] Overall, the tools are complex, leaving many implementations problematic from a privacy perspective.

The technology supporting digital identity credentials exists in a difficult grey area. If a service can see data, as it may during authentication and authorization moments, they can store it and use it, possibly correlate it, or even sell it at any future date. While single components may not themselves identify an individual, when they are combined from multiple systems and interactions, identification may happen.

This section takes a high-level look at some of the privacy-related issues affecting these credentials via the technology itself.

[90] The World Bank ID4D. "Practitioner's Guide." Accessed April 1, 2023. https://id4d.worldbank.org/guide/creating-good-id-system-presents-risks-and-challenges-there-are-common-success-factors.

[91] Waldman, Ari Ezra, "Cognitive Biases, Dark Patterns, and the 'Privacy Paradox'" (2020). Articles & Chapters. 1332. https://digitalcommons.nyls.edu/fac_articles_chapters/1332

[92] See for example the note in 4.7 Proofs (Signature) in "Verifiable Credentials Data Model v1.1," https://www.w3.org/TR/vc-data-model.

4.2.1 Intrinsic Limitations of Protocols

While the digital landscape is dependent on technology, technology cannot solve all the challenges any more than laws and regulations can protect for all use cases. Technology must support strict regulatory environments where all transactions must be logged, audited, and controlled, while also supporting consumer environments where transactions should be entirely at the discretion of the individual. Offline and remote scenarios are also challenging as any dependency on real-time validation is impossible. Technology can mitigate the risk of a credential being inappropriately used by a bad actor, but it cannot negate that risk entirely.

Expecting technology to perform moral judgements or culturally sensitive decisions leads us into the realm of artificial intelligence, an area that has its own issues with privacy that go far beyond the scope of this paper.

4.2.2 Biometrics Technologies

Biometrics, particularly facial recognition, are increasingly popular as a way to match an individual to their digital credentials.[93] The convenience for the individual, when everything works as the developers expect, is high. Governments often find facial recognition to be the simplest way for people to take advantage of the new online tools and services governments are offering, and also a powerful way to minimize fraud by tightly coupling something the person is to something they have. The accuracy of these systems, however, remains problematic. Verification services such as phone apps still struggle with the full range of the human phenotype. [94]

The convenience for individuals when authenticating to systems with biometrics is significant, but the technology comes with significant privacy concerns. In those scenarios where the biometric data leaves the device, collecting and storing the details of individual biometrics is a significant privacy risk if the data is not properly secured. There are even more concerns if the biometric data is used by third-party systems as the sole

[93] Shaheed, Kashif, Aihua Mao, Imran Qureshi, Munish Kumar, Qaisar Abbas, Inam Ullah, and Xingming Zhang. "A Systematic Review on Physiological-Based Biometric Recognition Systems: Current and Future Trends." *Archives of Computational Methods in Engineering* 28, no. 7 (2021): 4917–60. https://doi.org/10.1007/s11831-021-09560-3.

[94] Zukarnain, Z.A.; Muneer, A.; Ab Aziz, M.K. Authentication Securing Methods for Mobile Identity: Issues, Solutions and Challenges. Symmetry 2022, 14, 821. https://doi.org/10.3390/sym14040821

authenticator, checking the data against a central repository to determine if an individual is approved or explicitly disallowed in some manner.[95]

While not directly a privacy concern, the challenge in changing biometric data does lead to related concerns of usability and security. It is relatively easy to change a password; it is often more difficult to change biometrics. There is ongoing research on the concept of biohashing and revocable biometrics, but the extent of the use of these techniques by governments is unclear.[96]

In the U.S., there are no national-level privacy laws, nor national ones specific to biometrics. Individual states are passing their own laws for companies operating in their state. In Illinois, for example, the Biometrics Information Privacy Act, originally enacted in 2008, focuses on concerns regarding the abuse of biometrics and associated privacy implications. This act, however, excludes state and local governments and their contractors.

Even in Europe with the GDPR, member states may require different protections for biometric data.[97] There are also broad provisions that allow EU member states to process personal data without consent if there is a "national security," "defense," or "public security" concern, terms that are at best poorly defined.[98]

Ultimately, while biometrics are heavily used by governments to tie the credential with the individual, the details of their protections and the associated risk of their use is a major concern to many.

4.2.3 The Protocols of Authentication and Authorization

As noted above, governments issuing digital credentials are focused on a few specific protocols: SAML, OAuth and OpenID Connect, and Verifiable Credentials. When it comes to

[95] Bertocci, Vittorio. "A Tale of Two Biometrics Styles." Auth0 - Blog, March 10, 2023. https://auth0.com/blog/a-tale-of-two-biometrics-styles/.

[96] See for example Prabhu, D., S. Vijay Bhanu, and S. Suthir. 'Privacy Preserving Steganography Based Biometric Authentication System for Cloud Computing Environment'. Measurement: Sensors 24 (2022): 100511. https://doi.org/10.1016/j.measen.2022.100511 and Loh, Jia-Chng, Geong-Sen Poh, Jason H. M. Ying, Hoon Wei Lim, Jonathan Pan, and Weiyang Wong. "PBio: Enabling Cross-Organizational Biometric Authentication Service through Secure Sharing of Biometric Templates," November 10, 2020. https://eprint.iacr.org/2020/1381.

[97] Ross, Danny. "Processing Biometric Data? Be Careful, under the GDPR." International Association of Privacy Professionals, October 13, 2017. https://iapp.org/news/a/processing-biometric-data-be-careful-under-the-gdpr/.

[98] Human Rights Watch. "The EU General Data Protection Regulation," June 6, 2018. https://www.hrw.org/news/2018/06/06/eu-general-data-protection-regulation.

privacy implications however, these protocols vary in how they're documented or even understood by the protocol architects.

SAML was designed with privacy as a fundamental, documented part of the specification. Since the publication of SAML 1.0 in 2002, the standard included a separate document entirely focused on security and privacy.[99] This has been updated with the two successive versions of SAML (1.1 and 2.0).[100] It is one of the most robust treatments of privacy in any of the commonly used authentication standards.

For the OAuth family of specifications, developed within the IETF, a formal privacy consideration as per RFC 6793, "Privacy Considerations for Internet Protocols," is missing.[101]
This is likely in part because the original core specification included no identity information at all, being focused entirely on delegated authorization. That said, these specifications do include security considerations, and there are certainly privacy implications of the security of the specification leaves gaps, but even the RFC dedicated to the threats and security of the OAuth 2.0 model ("OAuth 2.0 Threat Model and Security Considerations" (RFC 6819)) does not directly refer to privacy beyond the following statement: "Note: Any implementation should consider potential privacy implications of using device identifiers."[102]

The OpenID core specification, created within the OpenID Foundation, does include a Privacy Considerations section, though most of the related specifications do not (the exception being "OpenID 2.0 to OpenID Connect Migration 1.0"). Having a privacy consideration section in the core of the specification is a positive action, though the nature of the specification itself limits some critical capabilities when it comes to all the facts of a robust privacy framework. OIDC transactions are point-in-time transactions, limiting the ability to incorporate non-functional factors into the specification. While consent and

[99] "Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML)." OASIS, 15 March 2015. https://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf.
[100] F. Hirsch et al. Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS SSTC, March 2005. Document ID saml-sec-consider-2.0-os. See http://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf.
[101] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, DOI 10.17487/RFC6973, July 2013, <https://www.rfc-editor.org/info/rfc6973>.
[102] See pg 58 of Lodderstedt, T., Ed., McGloin, M., and P. Hunt, "OAuth 2.0 Threat Model and Security Considerations", RFC 6819, DOI 10.17487/RFC6819, January 2013, <https://www.rfc-editor.org/info/rfc6819>.

choice as well as data minimization, two of the principles included in the OECD Privacy Guidelines, are included to some extent, other principles, including purpose legitimacy, collection limitation, use, retention, and disclosure, accuracy and quality, individual participation, and information security, fall out of scope. These areas are expected to be described in policy and other decisions outside the point of time of use.

The Verifiable Credentials specification, coming from the World Wide Web consortium, is another core specification that includes an extensive privacy considerations section.[103] As a newer specification in this family, receiving much of its attention from the work in the EU on digital wallets, the supporting material such as the implementation guidelines, do not contain any special note on privacy.

4.2.4 Verifying Data

A critical component to allowing people and organizations to trust identity information is verified claims. Verified claims provide assured identity information, but the details on how to share this information is still under development. The OpenID Foundation eKYC and Identity Assurance (eKYC & IDA) working group is focused on "developing extensions to OpenID Connect that will standardise the communication of assured identity information, i.e. verified claims and information about how the verification was done and how the respective claims are maintained."[104]

The ability to support verified claims is particularly relevant to privacy; it allows enough trust in the system that it should mitigate the perceived need to collect even more information to cross-check what is being asserted about the individual. Without the ability to programmatically verify information, government-issued digital credentials cannot successfully meet the diversity of uses they are expected to support. The work under discussion is not trying to address how organizations will use the data available in the credentials.[105] Instead, this technology would allow organizations to represent information they need as well as allowing them to comply with data minimization principles.

The relevant specifications are still under development; until they are completed and in use, this functionality remains a gap in the technology supporting these credentials.

[103] "Verifiable Credentials Data Model v1.1," https://www.w3.org/TR/vc-data-model.
[104] OpenID Foundation. "EKYC & Identity Assurance WG." Accessed April 1, 2023. https://openid.net/wg/ekyc-ida/.
[105] Fett, Daniel, "OIDC Advanced Syntax for Claims (ASC) - Transformed Claims & Selective Abort/Omit," presentation, 12 May 2021, https://danielfett.de/download/oidc-advanced-syntax-for-claims.pdf

4.2.5 Comparing the Policies in Technology

Not all organizations have the same rules when it comes to what kind of credentials they will accept. This is as much a problem of technology as it is legality. The Open Identity Exchange (OIX) is focused on what a full-scale trust framework needs to consider, from the policy to the technology. This includes how to deal with the many different constraints that may need to be applied when presenting information to an RP. The technical policy descriptions vary enough that verification and use of credentials across industries (e.g., healthcare, financial services, education) and jurisdictions becomes impossible.

While there are various open-source policy description languages, none include passing the policy descriptions from one entity to another.[106] The authors of the OpenID Foundation's eKYC & IDA Working Group's "Advanced Syntax for Claims" draft have looked at writing their own using Rego, JSONlogic and possibly others but are still discussing next steps.[107] Verification of the credential depends on the entity doing the verification, what information they are requesting out of the credential, and the format of their request. None of that can be shared today in a way that supports the basic principles of security and privacy.

Part of the limitation is an increasing dependence on advanced cryptographic algorithms that enable more granular sharing and validation of information. Development around selective disclosure in general and zero-knowledge proofs in specific has opened up some powerful possibilities for privacy. While enabled in several test implementations, these implementations require the new algorithms be supported in the device operating system and on hardware powerful enough to handle the math.[108]

There are other approaches that do not require advanced cryptography, specifically hash-based approaches as are being described in the IETF's OAuth working group draft, "Selective Disclosures for JWTs (SD JWTs)."[109]

[106] See De Coi, Juri Luca, and Daniel Olmedilla. "A Review of Trust Management, Security and Privacy Policy Languages." *Secrypt* (2008): 483-490 and World Wide Web Consortium. "PolicyLangReview - Policy Languages Interest Group," May 20, 2009. https://www.w3.org/Policy/pling/wiki/PolicyLangReview.
[107] Haine, Mark. "EKYC & IDA WG Report." *OpenID Foundation*. n.d. https://openid.net/wordpress-content/uploads/2021/09/OIDF_eKYC-WG-Update_Mark-Haine-Daniel-Fett.pdf.
[108] Bertocci, Vittorio, and Daniel Fett. "Daniel Fett on Privacy-Preserving Measures and SD-JWT." Auth0, September 29, 2022. https://identityunlocked.auth0.com/public/49/Identity%2C-Unlocked.--bed7fada/3bbcbab8.
[109] Fett, Daniel, Kristina Yasuda, and Brian Campbell. "Selective Disclosure for JWTs (SD-JWT)." IETF Datatracker, March 13, 2023. https://datatracker.ietf.org/doc/draft-ietf-oauth-selective-disclosure-jwt/.

4.2.6 Data Correlation and Re-use

The Use and Purpose Limitations found in the OECD Privacy Principles state that services should only collect the data they need for the purpose they state they are using it for. These concepts are included in several of the standards, laws, and regulations in the world. The gap comes, however, in interpretation. If an individual uses their government-issued digital credential for the purpose of travel, is it inappropriate for travel services to use that information to further enhance the individuals experience?

The line is not always clear. Organizations interested in staying on the right side of the law include what they are legally required to in their privacy statements and end-user license agreements, but those statements are notoriously difficult to read.[110] As individuals encounter new ways of being identified, authenticated, and authorized, they perceive new threats to their privacy they do not know how to address.

> *"However, emerging travel technologies such as biometric verification at airports require the collection, use, and storage of new types of information that are considered highly sensitive, such as face and retina images, fingerprints, and speech recognition (i.e., biometric data). At times, travelers may perceive that they did not have a choice to opt out from sharing their biometric data for processing at airports, or that they were not appropriately notified or asked to give consent in advance of collection and use of their biometric data (Street 2019)." – Athina Ioannou, Iis P. Tussyadiah, and Graham Miller, Journal of Travel Research.*[111]

As with many of the gaps in the area of digital identity in general and government-issued digital credentials in specific, this gap falls in an area that touches both the limits of technology and the constraints of current regulation.

[110] Zhang, Yibo, Tawei Wang, and Carol Hsu. "The effects of voluntary GDPR adoption and the readability of privacy statements on customers' information disclosure intention and trust." *Journal of Intellectual Capital* 21, no. 2 (2020): 145-163.

[111] Ioannou, Athina, Iis P. Tussyadiah, and Graham Miller. "That's Private! Understanding Travelers' Privacy Concerns and Online Data Disclosure." *Journal of Travel Research* 60, no. 7 (September 1, 2021): 1510–26. https://doi.org/10.1177/0047287520951642.

4.3 Protections Missing in Regulation and Standards

When it comes to government-issued digital credentials, privacy considerations are often held to literally a different standard than the private sector. This is both understandable and concerning; governments have very different requirements and responsibilities. The need for high levels of identity validation and verification with these credentials, combined with an expectation of securing people's data, makes implementing privacy protections uniquely challenging.

As an example where protections are defined in law but hold government agencies as out of scope, the Illinois Biometric Information Privacy Act (BIPA) only applies to private entities.[112] State or local government agencies or the court and its members (e.g., clerk, judge, or justice) are not included.[113] Alternatively, Singapore has an extensive Public Sector (Governance) Act (PSGA) laying out the requirements for security and privacy as they apply to government services. The U.S. NIST SP 800-63 falls in the middle, as it applies only at the federal level; states vary significantly in how they draft privacy legislation and whether it applies to government agencies at all.

Several of the standards and regulations have only gone as far as to specify in-person, on-device requirements. Describing the requirements and limitations when considering remote scenarios where data may need to leave the device on which it is stored are still in draft or under discussion as noted in the review above of ISO/IEC 18013-5 and ISO/IEC 27553-2.

4.3.1 India's Digital Personal Data Protection Bill 2022

Legislative efforts to support online privacy in India include a new Digital Personal Data Protection bill under consideration by India's parliament. This is the second effort at such a bill; Parliament dropped the earlier version in August 2022. With the Aadhaar system providing credentials to over a billion people, the concerns about how the personal data from that system and other online services will be used must be addressed in part by legal protections that give individuals recourse when it comes to protecting their data.

[112] Institute for Legal Reform. "ILR Briefly: A Bad Match: Illinois and the Biometric Information Privacy Act - ILR." ILR, October 12, 2021. https://instituteforlegalreform.com/research/ilr-briefly-a-bad-match-illinois-and-the-biometric-information-privacy-act/.

[113] "Biometric Information Privacy Act." Illinois General Assembly, October 3, 2008. https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

All legislation is the result of compromise, and the Digital Personal Data Protection bill still has privacy advocates arguing for greater protections from the government itself.[114] The issue of government surveillance remains a significant concern.[115] The fact that the bill explicitly excludes offline and paper-based data collection leaves the question of whether digitized paper records are protected as well.[116]

The bill is designed on several principles common in other regions' privacy legislation and the OECD Privacy Guidelines, including lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, and accountability. But how those principles are applied when it comes to the government monitoring itself or that grey area of digitized forms is definitely a gap in the proposed protections.

4.3.2 Singapore's Personal Data Protection Act and the Public Sector (Governance) Act

Singapore is one of the few nations that explicitly lays out the privacy and security requirements for the government in a clearly documented way. PDPA sets out the legal framework for data protection responsibilities in the private sector.[117] The PSGA is the corresponding legal framework for the public sector.[118] The levels of control are different, with the PDPA focusing on consent and the PSGA touching on more aspects of cybersecurity.[119] The fact that there are separate legal frameworks is both a positive, in that it makes the privacy landscape for Singapore more transparent, and negative, in that there are significant disparities between public and private sector privacy protections.

[114] Sherman, Justin. "India's New Data Bill Is a Mixed Bag for Privacy." Atlantic Council, November 23, 2022. https://www.atlanticcouncil.org/blogs/southasiasource/indias-new-data-bill-is-a-mixed-bag-for-privacy/.
[115] Mathi, Sarvesh. "Data Protection Bill Legitimises Surveillance, Govt Has No Intent of Reforms: Stakeholders #NAMA." MediaNama, December 20, 2022. https://www.medianama.com/2022/12/223-dpdp-bill-2022-enables-govt-surveillance-discussion/.
[116] Nandle, Ravin. "India's Digital Personal Data Protection Bill 2022: Does It Overhaul the Former PDPB?" International Association of Privacy Professionals, November 22, 2022. https://iapp.org/news/a/indias-digital-personal-data-protection-bill-2022-does-it-overhaul-the-former-pdpb/.
[117] Lim, Chong Kin. "Singapore - Data Protection Overview." OneTrust DataGuidance, May 2022. https://www.dataguidance.com/notes/singapore-data-protection-overview.
[118] Government of Singapore, Smart Nation and Digital Government Office (SNDGO). "Government's Personal Data Protection Laws And Policies." Accessed April 1, 2023. https://www.smartnation.gov.sg/about-smart-nation/secure-smart-nation/personal-data-protection-laws-and-policies.
[119] Singapore Management University Newsroom. "Where Does Privacy Stand in This Age of Social Media and Data Breaches?," May 13, 2019. https://news.smu.edu.sg/news/2019/05/13/where-does-privacy-stand-age-social-media-and-data-breaches.

As is often the case when it comes to government services, the prevalent theme is a concern regarding surveillance.[120] The PSGA allows extensive data sharing between government departments without requiring use consent or even knowledge. There appears to be no legal resource for an individual to learn what data has been collected nor how it has been used by the government. With Singpass serving as a ubiquitous credential for so many services, the amount of data potentially collected is significant.

4.3.3 GDPR, NIS2, and eIDAS

GDPR, NIS2, and eIDAS 2.0 all touch on personal data, though privacy is only one of several design considerations guiding the regulations. The GDPR is often pointed to as the 'gold standard' of privacy regulations in the world as it offers European member state citizens and residents extensive privacy protections. NIS2, however, is more focused on increasing the resilience of critical digital infrastructure. Requirements in NIS2 focus on system-level security rather than data-level protection, which may result in contradictory requirements that impact individual data privacy.[121] And the regulation focusing on digital identity, eIDAS 2.0, balances the restrictions imposed on third-party data sharing by the GDPR by building a data sharing model owned by the data subject.

With these and other EU regulations all influencing the identity space and, perforce, government-issued digital credentials, there is significant risk of contradictions and gaps in the privacy landscape.

From a technical perspective, the focus on the national wallets suggests that the wallet itself has become a single point of failure. If the individual cannot use the wallet for whatever reason, they may have to resort to less privacy-enhancing processes such as sharing copies of a physical driver's license or passport. There is also the point that while the technology housing the wallet is not specified, the mobile device vendor becomes another component in the identity ecosystem (along with the government issuer, the relying party or verifier, and even the individual) that must be considered when designing a verifiable trust model.

[120] Choo, Julia, and Anngee Neo. "The Use and Abuse of Personal Data by the PAP Government." New Naratif, June 7, 2022. https://newnaratif.com/the-use-and-abuse-of-personal-data-by-the-pap-government/.
[121] For more on how NIS2 and GDPR relate to each other, see Perray, Romain, and Pilar Arzuaga. "Regulating Cybersecurity across the EU and the UK - McDermott Will & Emery." McDermott Will & Emery, January 2023. https://www.mwe.com/insights/regulating-cybersecurity-across-the-eu-and-the-uk/.

4.3.4 U.S. Federal and State Privacy Laws

The U.S. is one of the few countries that does not have a national, comprehensive privacy law. Instead, laws focus on specific information or sectors, such as health or financial data. Different states step into this gap, such as California, Utah, Colorado, Virginia, and Connecticut, but efforts are uncoordinated and inconsistent. The International Association of Privacy Professionals (IAPP) offers a U.S. State Privacy Legislation Tracker for individuals interested in tracking this complicated landscape.[122]

An Example of Introducing New Privacy Risks

Governments collect a large amount of data about their citizens. In fact, they are the source of truth for birth dates, gender assigned at birth, citizenship, and more. All of that information is necessary to provide the strong levels of assurance regarding individual identity that governments are known for. This data is used for everything from social services, diversity, equity, and inclusion (DEI) initiatives, financial services, and more.

Collecting this data is both necessary and risky. In a paper presented at Blackhat USA 2019, authors James Pavur and Casey Knerr described how the "Right of Access" process within the GDPR has the potential to result in data theft by exposing sensitive information to unauthorized third parties.[123]

The right of access included in the GDPR allows EU residents to send subject access requests (SARs) to most organizations. Those organizations are required to respond within one month with a copy of all the personal data that organization holds on that resident. The GDPR does not specify beyond stating that the organization may employ "all reasonable measures to verify the identity of a data subject who requests access" (Rec. 64). The GDPR does not offer any further guidance on organizations that are expected to verify the identity of the requester. In fact, the GDPR further states that organizations cannot collect more data to help them identify the individual in the case an SAR is submitted.

This is a significant privacy risk that has been introduced by legislation designed to protect an individual's privacy.

[122] Anokhy Desai. "US State Privacy Legislation Tracker." IAPP Resource Center, March 31, 2023. International Association of Privacy Professionals. Accessed April 1, 2023. https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.

[123] Pavur, James, and Casey Knerr. "GDPArrrrr: Using Privacy Laws to Steal Identities." Blackhat USA 2019 Whitepaper, 2019. https://i.blackhat.com/USA-19/Thursday/us-19-Pavur-GDPArrrrr-Using-Privacy-Laws-To-Steal-Identities-wp.pdf.

5 Recommendations for Scaling to the Future

Governments' promise a wealth of benefits from digital transformation. From economic growth to improved efficiency and transparency in government services, digital transformation demands full speed ahead to live up to the dream. At a more detailed level, by issuing high-quality verified credentials, governments promise compelling outcomes, including:

- support for individual control over their own data disclosure.
- requirements for data minimization by all parties.
- laws and regulations demanding relying party accountability.
- possibility of audit logs of transactions and ability to assert rights (CCPA, GDPR).
- minimization of fraud along with associated cost savings.
- potential for extensibility to other domains outside of direct government use cases.

These promises make for worthwhile goals, but they cannot be done independently of each other and are by no means certain outcomes. They exist in a set of tradeoffs that see governments struggle to balance the needs of greater efficiency, the expectation of digital services from a changing demographic, contradictory individual behaviors, and demands for privacy.[124] Technology, in turn, is working to balance those same needs against the additional fact of basic limitations around what's possible for the protocols to support. The end result is that both the government and private sector are moving towards more centralized storage of identity data rather than distributed models in an attempt to give them control over an incredibly complex environment.

Regulation often demands behaviors (e.g., collection of consent) that make bringing services in the private sector in-house rather than relying on external information, even government-issued digital credentials and their wallets, a safer option.[125] In addition, the

[124] See for example page 120 of the United Nations. "E-Government Survey 2022: The Future of Digital Government." United Nations, 2022. https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2022.

[125] A general example of this is the work-in-progress of browser vendors as they look to intermediate web-based authentication and authorization flows in order to register user consent for a federated login transaction.

increasingly complex collection of technical standards and specifications required for interoperability across organizational boundaries is itself a significant burden to any organization, including governments, trying to operate in a digital environment.

Regulatory demands, complex technological implementations, cross-border complexities: the end result is an experience that degrades an individual's trust in the system and opens the door to bad actors who take advantage of the chaos. How can governments, civil society, standards organizations, and developers work together to bring order to the system? How can the stakeholders in this multi-way trust model offer simpler solutions for the individual when the requirements are so complex? This section looks at some of the possible ways the privacy landscape can be improved for government-issued digital credentials.

5.1 The Basics of Security and Privacy

There are several concepts described in the OECD Privacy Principles and ISO/IEC 29100, described earlier in this document, that should serve as the foundation of every discussion about privacy within digital systems. These principles are not new, and yet governments and private-sector organizations tend to either reinvent them or pick-and-choose what they want to incorporate into their legal and technical systems.

When it comes to government-issued digital credentials, these principles should be treated as the basic, foundational principles that are and incorporated in the earliest stages of planning and design.

Governments should review current cybersecurity best practices, such as what are described in NIS2, the NIST Cybersecurity Framework, and the proposed the EU Cyber Resilience Act.[126] in order to comply with the OECD Security Safeguards Principle, which states, “Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.” How they protect the personal data in their systems will be one of the most critical measures of success of their services.

See the work under discussion in the W3C Federated Identity Community Group. World Wide Web Consortium. “Federated Identity Community Group.” Accessed April 2, 2023. https://www.w3.org/community/fed-id/.

[126] See NIS2 http://data.europa.eu/eli/dir/2022/2555/oj, the National Institute of Standards and Technology. “Cybersecurity Framework | NIST.” NIST. Accessed April 2, 2023. https://www.nist.gov/cyberframework, and the European Commission. “Cyber Resilience Act.” Shaping Europe’s Digital Future, September 15, 2022. https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act.

Governments should also keep in mind that they are the most significant data controller in the digital ecosystem, and as such, should hold themselves answerable to the Accountability Principle ("A data controller should be accountable for complying with measures which give effect to the principles stated above."

The remaining principles described by the OECD also apply, but additional consideration regarding their implications is required.

5.1.1 Individual Agency

Consent and user control is an item strongly addressed in regulation for private issuance and use of digital credentials, but perhaps not to the effect regulators have intended it to be.[127] Consent is also covered in the OECD's Collection Limitation, Use Limitation, and Individual Participation Principles. Government issuance and use of digital credentials raise the bar for when and how consent is requested, even for government services. Governments must consider what information they actually require from an individual for the different actions they might take in a system, rather than focus on what information they want to enable other, possibly unrelated actions.

For example, governments might consider a consent-management service for data disclosure that allows individuals to set defaults for data release such that services would not need to request further consent if what they are asking for and what the individual allows align. Alternatively, they could require consent records be implemented in each wallet on device (something that has made its way into standards such as ISO/IEC 18013-5). If the individual's defaults do not align with the service's requirements, the service could be required to explain what information they are requesting and why and give the individual the opportunity to choose a different path. The individual should have the option for selective disclosure of their information to minimize their digital footprint.[128]

[127] For more information, see Cate, Fred H. and Mayer-Schönberger, Viktor, "Notice and Consent in a World of Big Data" (2013). Articles by Maurer Faculty. 2662. https://www.repository.law.indiana.edu/facpub/2662.
[128] See for example AAMVA's mDL implementation guidelines and the specific guidance on Data Minimization and Selective Disclosure. AAMVA. "Mobile Driver's License Implementation Guidelines 1.2 - American Association of Motor Vehicle Administrators - AAMVA," January 2023, pp 27-29. https://www.aamva.org/assets/best-practices,-guides,-standards,-manuals,-whitepapers/mobile-driver-s-license-implementation-guidelines-1-2.

The individual must have agency, but they must also not be burdened with unnecessary choices. Defaults should always be sensible and minimize the requests being made of the individual, and the best choice for privacy should always be the easiest one.

5.1.2 Systemic Transparency

Coupled with the concept of user control, governments are building transparency in their systems to encourage trust. In some cases, they are doing this by showing what their services are doing down to the layer of the code itself.[129] In others, they are relying on documentation and service tools that individuals can read and use to see what the government exposes regarding their systems. This brings into play the Openness and Purpose Specification Principles from the OECD, and yet, these principles are being handled very differently.

For example, In the Aadhaar system, residents can review their digital identity's authentication history via a website. But the Aadhaar technology itself is run as a centralized, proprietary system.[130] Singpass, on the other hand, offers its API source code to the world in a GitHub repository.[131]

The U.S. state of California is in the process of reviewing cybersecurity audit requirements that may become a strong part of their efforts towards transparency.[132] The GDPR, conversely, has no formal audit requirements at all.

With third parties using government-issued digital credentials, those relying parties should also be subject to reviews and held accountable to when and how they use and retain data. In Singapore, relying party accountability is a prominent component of the Singpass system.[133] In Italy, every new relying party is reviewed and charged a small fee before being allowed to access the system.

[129] See Government of Singapore. "Singpass." GitHub. Accessed April 2, 2023. https://github.com/singpass.
[130] Privacy International. "ID Systems Analysed: Aadhaar," November 19, 2021. https://privacyinternational.org/case-study/4698/id-systems-analysed-aadhaar.
[131] "Singpass." https://github.com/singpass.
[132] State of California. "Frequently Asked Questions (FAQs) - California Privacy Protection Agency (CPPA)." Accessed April 2, 2023. https://cppa.ca.gov/faq.html.
[133] Personal Data Protection Commission Singapore. "PDPC | Accountability." Accessed April 2, 2023. https://www.pdpc.gov.sg/accountability.

5.1.3 Data Minimization

A fundamental security best practice further enshrined in regulations around the world and the OECD Data Quality Principle. The GDPR, for example, requires that data controllers "should limit the collection of personal information to what is directly relevant and necessary to accomplish a specified purpose." Of course, the interpretation of what is directly relevant and necessary is open to interpretation; the enforcement mechanisms on both the legal and the technical sides are inconsistently applied or completely lacking. Still, one of the most powerful ways to protect an individual's data privacy is to not collect their personal data at all.

Governments are in a unique position of being the source of truth to a large amount of personal data. Birth records, legal names, and citizenship are just a few examples of data that governments generate for citizens and residents of their countries. However, they are also likely to collect even more data that is not necessarily in their purview. As government agencies collect data such as race, gender, and sexual orientation in order to evaluate whether or not they are supporting diversity and equity, that data becomes a source of information that may be used for other purposes if those purposes are declared important by the government itself (e.g., public safety).[134]

The U.S. National Institute of Standards and Technologies (NIST) has documented guidelines for the U.S. Government in NIST Special Publication 800-53 "Security and Privacy Controls for Information Systems and Organizations."[135] This provides all U.S. government agencies with strict guidelines on data collection and handling.

Singapore focuses on a variety of principles and implicitly addresses data minimization in their "Privacy-conscious design" principle, "Be assured of your privacy when transacting on-the-go by easily hiding sensitive data in your Singpass app profile."[136] The information is hidden from services requesting components of an individual's Singpass data, but a

[134] See for example the information on LGBTQ+ and points on data collection in Executive Office of the President. "Advancing Equality for Lesbian, Gay, Bisexual, Transgender, Queer, and Intersex Individuals." *Federal Register - the Daily Journal of the United States Federal Government*, June 15, 2022. https://www.federalregister.gov/documents/2022/06/21/2022-13391/advancing-equality-for-lesbian-gay-bisexual-transgender-queer-and-intersex-individuals.

[135] Force, Joint Task. "Security and Privacy Controls for Information Systems and Organizations." CSRC, December 10, 2020. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

[136] Government of Singapore. "Singpass - Principles." Accessed April 2, 2023. https://www.singpass.gov.sg/main/principles/.

significant amount of data from bank account information and more is still stored in the service.

The guidelines offered by the European Data Protection Board (EDPB) provide a good starting place for the design elements that must be considered for a good start to approaching to data minimization.[137]

More, however, should be done, to support data minimization at scale. Governments, civil society, and organizations agree what the minimum set of data is for a given transaction type. For example, documenting that banks should only verify the government-issued digital credentials are authentic, collect the individuals name and date of birth, and affirm that the credential is not expired. No other information may be collected.

If each relying party is certified and registered according to what information they may collect, the technology may be able to enforce data minimization in accordance with whatever laws and regulations have been established. Third-party audits via a government-private sector partnership must be a regular component of verifying compliance to confirm the protection of personal data.

5.1.4 Advancing Cryptography

To complement the regulations that promote data minimization, consent, and other basic principles, there must be increased development in tools like zero-knowledge proofs and selective disclosure. As noted earlier in the paper, these technologies, which provide the means to release only a subset of data from a credential, rely on advanced cryptographic algorithms. These algorithms are challenging to implement and are often associated with the need for a specific credential format.[138] So, while the technology exists, it is not widely adopted. Everything from operating system vendors, computer hardware manufacturers, and standards developers must engage in making the necessary cryptography broadly available.

[137] European Data Protection Board. "Adopted 1 Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0," October 20, 2020, pp21-23. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

[138] "Daniel Fett on Privacy-Preserving Measures and SD-JWT." https://identityunlocked.auth0.com/public/49/Identity%2C-Unlocked.--bed7fada/3bbcbab8.

5.2 Addressing Ongoing Concerns

As the basics of security and privacy are built into the systems using government-issued digital credentials, there are systemic concerns that governments and technologists must address in order to bridge the gaps between the privacy individuals demand, the abilities of the technology, and the tradeoffs being made by governments.

5.2.1 Surveillance

Every article and research paper that considers privacy and government systems includes the concern of government surveillance. In some cases, governments such as what is observed in Singapore are quite open about the fact that they are using any and all data they collect to bring about their vision of a more safe and efficient society.

If governments are to improve their support of a just democracy and supporter of human rights, they must do more to demonstrate their support for and adherence to basic privacy and security principles, especially for their own systems and services.

5.2.2 Diversity, Equity, and Inclusion

Diversity, Equity, and Inclusion (DEI) have a close relationship with privacy, though they are unique enough in their own right to warrant a separate study. The use of government-issued digital credentials depends on many things that are not universal: access to technology, ability to use technology, or even desire to use technology.

DEI implications also tie back to concerns regarding surveillance. Individuals from minority or otherwise marginalized groups share concerns that use of government services, including use of a digital credential, will result in tracking and negative action by the government.

As one example of where this is a relevant concern, DEI and privacy advocates point to the issue of algorithm exclusion. As governments become more advanced in the use of AI to help make decisions around access to services, algorithmic exclusion is growing as a concern. Algorithmic exclusion, defined by Dr. Catherine Tucker as “outcomes where

people are excluded from algorithmic processing, meaning that the algorithm cannot make a prediction about them," because of bad or missing data.[139]

When government services rely on digital credentials, then those individuals that cannot obtain those credentials are likely to be excluded from benefiting from those government services.

While efforts such as the new equity guidelines in draft NIST SP 800-63-4 attempt to prevent this type of exclusion, DEI issues remain something that must be addressed by society at large. Governments and technologists have opportunities to do more to improve these issues by engaging in efforts to design equity into their regulations and consider how to improve technology to support a more diverse user base.

5.2.3 Single Points of Failure

The expectation that these credentials have a certain level of validation results in the government collecting large amounts of personal data. While perhaps obvious, a corollary to that is a concern about how the government protects that data. In the case of the Aadhaar system, a breach of the centralized collection of data resulted in the exposure of over a billion records. In other government system breaches, biometric data was compromised.

Governments must do everything possible to protect the data in their care, avoiding single points of failure and, when storing biometric data, being careful to apply biohashing to the information (see section 4.2.2 Biometrics Technologies for more information on biohashing).

5.2.4 Inappropriate Use by Legitimate Actors

Even where governments are included in regulation requiring compliance to privacy laws (something that is by no means universal) there are always powerful exceptions included under the banner of public safety and/or national security. Depending on the administration in power, the line between legitimate action and abuse is fluid. This concern reflects some of the issues in the area of sustainable protections and concerns regarding government surveillance.

[139] Tucker, Catherine. "Working Paper Algorithmic Exclusion: The Fragility of Algorithms to Sparse and Missing Data." The Center on Regulation and Markets at Brookings, February 2023. https://www.brookings.edu/wp-content/uploads/2023/02/Algorithmic-exclusion-FINAL.pdf.

There must be ways to hold governments accountable for their use of the personal data they collect as their credentials are used, which in turn requires transparency in the system so that individuals and society are aware of that use.

5.2.5 Sustainable Protections

Governments change. Elections, coups, and other actions see changes that will take a country or region from one political system or party to another. Laws that may exist in one regime may be reversed or abused in another. Unfortunately, these are the risks associated with all government systems; they can and will change over time, and not always in ways that improve the lives of their citizens and residents. So while making sure that laws and regulations support individual privacy, particularly with regards to digital identity, that will never be sufficient on its own.

This is why technology must evolve with regulation so that one can serve as the balance and control to the other. The technological standards and tools mentioned in this paper require additional resources, including both technologists as well as civil society members, in order to advance their efforts with greater speed and with more viewpoints represented.

Non-government organizations (NGOs) like the OECD, the United Nations, and the World Bank, as well as organizations such as the Secure Identity Alliance (SIA), the Global Legal Entity Identifier Foundation (GLEIF), the OpenID Foundation, and the World Privacy Forum must engage with all parties in the multi-stakeholder trust model in order to guide solutions that will work globally and in a way that buffers legal changes that degrade privacy protections.

5.3 Getting Ahead of Emerging Concerns

In addition to the ongoing concerns being discussed by governments, civil society, and technologists, new concerns are emerging as technology evolves. The use of artificial intelligence to make sense of the ever-increasing quantity and use of data is a growing field that touches all identity systems found in governments and the private sector. All stakeholders in the identity ecosystem need to consider these new issues and get ahead of bridging the gaps these introduce. This is highlighted in particular by the expansion of war into the digital arena.

5.3.1 Digital Warfare

Most, if not all, privacy laws and regulations include a provision that moves privacy in abeyance in the case of public safety. This is never more obvious than when a country is at war.

In a paper by Lothar Fritsch and Simone Fischer-Hübner, "Implications of Privacy & Security Research for the Upcoming Battlefield of Things," they focused on the future of privacy over the next 25 years when considered against "the Battlefield of Things."[140]

Systems can be designed in a way that supports the needs of military engagement while still complying with many of the basic security and privacy features noted in this paper.

> *"Data authenticity is an increasingly vital societal concern, and being able to collectively maintain a database without the need for central trust is, therefore, highly relevant. Similarly, centralised systems without adequate protection are single points of failure. Trust in sensor measurements as well as coordinated implementation of operations are critical for defence and civil security. Ensuring and documenting system consensus, algorithmic accountability, and verification of correct function of components will be important features of connected objects and their control systems. Secure logging technology may help investigate anomalies while preserving operation confidentiality." – L. Fritsch and S. Fischer-Hübner, Journal of Information Warfare [141]*

The overlap of private sector and military technologies (e.g., autonomous drones) suggests that privacy and security considerations must be built into all facets of society.

5.3.2 Deepfakes

Deepfakes, those realistic images and videos created using artificial intelligence and machine learning (AI/ML), are a growing threat on the digital landscape. With the advances in AI/ML technologies, deepfakes are turning up in fraud and forgery cases and proving to be a challenge to law enforcement.[142]

---

[140] Fritsch, L., Fischer-Hübner, S. (2019). Implications of Privacy & Security Research for the Upcoming Battlefield of Things. Journal of Information Warfare, 17(4). Available at https://www.diva-portal.org/smash/get/diva2:1306652/FULLTEXT02

[141] ibid , pp 78.

[142] Frederick Dauer, "Law Enforcement in the Era of Deepfakes," *Police Chief Online*, June 29, 2022.

It is not hard to imagine the technology used to develop deepfakes being used to conduct criminal activity in a remote credential usage scenario (e.g., the use cases being used for ISO/IEC 27533). Even as technical trust is advancing in efforts such as the OAuth Selective Disclosure efforts and OpenID for Verifiable Presentations, other technologies are evolving to find other ways to get around their protections.[143]

5.4 The Role of Civil Society

Civil society offers expertise and passion to both governments and standards development organizations to fill knowledge gaps in their laws, policies, and specifications. As noted earlier with the Privacy Considerations for Internet Protocols callout, the people writing the code (either technical or legal) often have the best of intentions, but they do not have the depth of expertise in the privacy space to address those considerations sufficiently.

The IAPP regularly responds to government consultations, as does the Electronic Privacy Information Center (EPIC). Privacy International, the Electronic Freedom Foundation (EFF), and several other civil society organizations focused on privacy are quite active in this area. This is a critical component of educating and advocating for privacy in the government context. These organizations are often less active, however, with technical standards development. This needs to change.

One avenue for that change might be the Internet Research Task Force's Privacy Enhancements and Assessments Research Group (pearg).[144] As a partner organization to the IETF, the Internet Research Task Force (IRTF) supports research into some of the more challenging problems facing the Internet. While the IRTF is not a standards-setting organization, with sufficient engagement, it may provide another way privacy advocates can inform the standards-setting process.

6 Conclusion

As governments lean into digital transformation and offer high-quality, government-issued digital credentials to their constituencies, they must consider privacy through the lens of

[143] "Selective Disclosure for JWTs (SD-JWT)," https://datatracker.ietf.org/doc/draft-ietf-oauth-selective-disclosure-jwt/ and "OpenID for Verifiable Credentials," https://openid.net/openid4vc/.
[144] "Privacy Enhancements and Assessments Research Group (Pearg)." Accessed April 1, 2023. https://datatracker.ietf.org/rg/pearg/about/.

the technologically possible and in the design of their laws and legislation. When considering how to protect society, governments must also remember society is made up of individuals who deserve both protection and agency to make decisions and feel safe in their activities online. Individuals and society as a whole are concerned about how governments will use the data they are perforce being entrusted with. It's up to governments to address those concerns.

Technology has the role of making privacy in an online world possible. Through protocol design, hardware and software advances, and cryptographic algorithm evolution, technology provides the tools to enable a more privacy-enhancing environment. Considering those tools in a purely neutral scenario, ignoring the threats of how they may be misused or abused in ways that impact privacy, invites new privacy risks that may have been avoided. It's up to technologists to incorporate privacy awareness into the core of their designs.

Given the scope of how these credentials are used in the world today, understanding the full breadth of privacy implications is an enormous challenge. Civil society has a deep understanding of the privacy landscape and is willing to engage, particularly with governments. That engagement is necessary, but it is not sufficient. Civil society must engage in technological development as well to help technologists know what they don't know now in the privacy landscape.

And, finally, individuals themselves have a role in helping improve this system. While it is up to the governments, the services, and the technologists to provide clear, actionable, and straightforward choices, individuals will need to take advantage of the choices available to them.

This paper has only touched the tip of the possibilities in this space. There are more governments issuing credentials to their constituencies. The technologists are constantly at work developing new protocols and tools. Civil society is engaging around the world on issues of privacy and related issues. Each section has hopefully inspired thought and will encourage more in-depth discussion as we all grapple with the incredibly complex environment of government-issued digital credentials and the privacy landscape.

7 Appendix A: Text of the OECD Privacy Principles

Copied from https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

Collection Limitation Principle

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up to date.

Purpose Specification Principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

a) with the consent of the data subject; or

b) by the authority of law.

Security Safeguards Principle

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence

and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

13. Individuals should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them;

b) to have communicated to them, data relating to them

i. within a reasonable time;

ii. at a charge, if any, that is not excessive;

iii. in a reasonable manner; and

iv. in a form that is readily intelligible to them;

c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle

14. A data controller should be accountable for complying with measures which give effect to the principles stated above.