



Horizon 2020 Programme
DG CNECT
Next-generation Internet



Project acronym: **PaE:CG**

Project title: **Privacy-as-Expected: Consent Gateway**

Partners: **Trinity College Dublin (TCD), OpenConsent Ltd., Birmingham City University (BCU)**



Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin



BIRMINGHAM CITY
University

D2 Final Technical Deliverable

Authors:	Harshvardhan J. Pandit (TCD), Dave Lewis (TCD) Mark Lizar, (OpenConsent), Salvatore D'Agostino (OpenConsent), Vitor Jesus (BCU), Shankar Ammai (BCU), Junaid Arshad (BCU)
Submission date:	2021-07-12
Dissemination level:	Public
DOI:	https://doi.org/10.5281/zenodo.5086239

Abstract: This document represents the final (combined) deliverable for the outcomes of the Privacy as Expected: Consent Gateway (PaE:CG) project. It outlines the project's main deliverables, which consist of: (1) a strategy and vision to offer internet users Consent Receipts and (2) software demonstrating the developed concepts.



Disclaimer

The sole responsibility for the content of this publication lies with the authors. It does not necessarily reflect the opinion of the European Commission. The European Commission is not responsible for any use that may be made of the information contained therein.

Copyright

This document may not be copied, reproduced, or modified in whole or in part for any purpose without written permission from the NGI Consortium. In addition, an acknowledgement of the authors of the document and all applicable portions of the copyright notice must be clearly referenced. All rights reserved.

This document may change without notice.

Table of contents

Rationale and Motivation	4
The 2 Global Privacy Challenges:	5
Usable Privacy & Rights Accessibility	6
The Challenges	6
Data Sovereignty on the Internet	6
Solution: Embedding access to privacy as expected	7
Use-cases	9
Architecture	9
Use-Cases of the proof-of-Concept	11
Implementation	15
User's Browser Extension	15
Web Server Module	23
Consent Gateway	28
Consent Receipts	31
Evaluation	37
Project Outcomes	38
Final Technical Report (this deliverable)	38
Open Source Software	38



Contributions to ISO/IEC 27560	38
Kantara, Advanced Notice and Consent Receipt Working Group	39
W3C Data Privacy Vocabulary CG	39
Schema.org	39
Workshop on Consent	40
Privacy as Expected (for Parental Consent) - Workshop on Global Code of Conduct for Parental Consent	40
Publication of Research Outputs	40
Future Work	41
Technical Developments	41
Future usability with GDPR	42
Laws, Standards & Technical Communities	44
Annex - Technical Communities	44
Semantic Terms Mapped	45
ISO/IEC 29184 Online Privacy Notice and Consent	45
Semantic Terms Mapped	45
W3C Data Privacy Vocabulary Controls Community Group (W3C DPV CG)	46
OASIS COEL - Classification for Everyday Living	47
Trust over IP: Notice & Consent Task Force	47
Blinding Identity Taxonomy: Kantara Initiative	48

1 Rationale and Motivation

The rationale to provide people with meaningful transparency is inspired by long term objective to evolve privacy and surveillance notices for human controlled consent grants and controls for system permissioning.

Moving past tick box terms and policies that do not provide proof of knowledge, which is required for informed human consent. Online the expectation that people will read linked policies before using a digital service, providing instant access is unreasonable, especially since $\frac{1}{3}$ of Internet service users are Children. Not legally allowed to permission surveillance capitalism without parental consent.

This project objective is to demonstrate an international alternative which dramatically increases the usability and access of privacy rights in Online environments, as well as value of personal data and meta data for people. A project that makes transparent and accountable surveillance capitalist services so the Next Generation Internet can move forward to operate with dynamic data control and permissioning. One in which meaningful consent is withdrawn per context, (many services) not permission required to be set on a per service basis.

An alternative Open Privacy Notice Alternative, to cookie pop-ups, built for the Individual to see what privacy they have (with a glance), reversing the burden of notice to the Data Controller, providing the tools people need to see a protect their own data on and offline in context.

An objective that resumes the original call for collaboration in the development and implementation of Open Notice standards that scale jurisdictions as well as the Internet.

Introducing: The PaE:CG (Privacy as Expected Consent Gateway) project, developed to engineer a much more performative alternative to cookies and pop-ups. By providing people with the tools to generate their own records using standards that codify best practices for Meaningful Consent. Which is essentially consent people themselves generate, control and can find trustworthy.

What is Privacy as Expected (PaE)

Privacy as Expected, refers to reasonable expectation of privacy that is entrenched in privacy law and rights, the basis of the 4th amendment in the US, Article 8 Human Rights Act in the EU, and echoed in legal decisions through privacy regimes all over the world. This expectation of privacy is critical for trustworthy use of personal data and data governance. At its core it is a legal protocol for generating proof of notice records and consent receipts, used to enhance privacy notices and automate access to privacy rights information.

PaE like the legal tests for determining what is fair and reasonable, extends privacy regulation with an open standard digital privacy notice record, which people themselves (or their user agent) create in order to generate consent/rights receipts.

Privacy as Expected is a much more intuitive signalling protocol for people (than terms and conditions) as the reasonable expectation of privacy is determined by the purpose, not terms and conditions. A purpose that is intuitive to the service, that people can understand.

The Consent Gateway component of this project provides additional Privacy Assurances for the Privacy as Expected protocol through an API that witnesses the claims in a consent receipt to sign the proof of notice once verified.. Meanwhile, the consent receipt captures the legal entities as well as the relationship context/preferences so that a service can automatically see the state of consent and permissions, without needing cookie pop-up banners, or requiring people to read contracts and privacy policies, but instead, provides people with direct access to privacy requesting privacy rights information. .

Useful, for example, to streamline online service experiences, and to replace the need for services to place records like cookies on a persons device. With the Consent Gateway the interactions, semantics of a PaE notice are assessed for conformance to standards, as well as access to privacy rights information, access and remedies.

The Consent Gateway is accessible with an API that is used to cryptographically witness the notice assertions of the Data Subject's capture of privacy notices and policies with a consent receipt. and to sign a consent receipt to provide proof of notice. Providing all privacy stakeholders with evidence of a valid state of consent and an auditable record for privacy compliance and rights administration.

Article 12 1-8 in the GDPR,¹ in particular ensure Article 13.1(a), and 14.1(a) Controller Identity and contact information are operational for use to validate a consent so that it is usable as evidence of access to privacy rights information.

Once identified, and notice is verified, GDPR Recital 47 can be applied with PaE protocol to assert privacy rights that supersede the legitimate interests of the Data Controller when privacy is not expected. Article 11, and Recital 51, stipulate public access to 'provided' privacy rights information, without having to provide digital identifiers. And critical for a universal PaECG signal, the use of icons and signals to indicate the active state of privacy control and accountability (GDPR Article 12, Recital 60 and 166). For example, if there is a data breach, a disclosure should/must be automatically provided using the PaE protocol, prior to the next use of a service.

PaE signalling is accomplished through semantically specified implementation of the two main project components. The first is the PaECG protocol implemented by identifying the legal, technical, and jurisdictional infrastructure required for PaE signalling to be active.

The second component, the Consent Gateway(CG), verifies the Data Controller by witnessing the privacy controller identifiers and privacy notice twin for the web service.

The Consent Gateway API is used to cryptographically sign a consent receipt to establish proof of privacy notice knowledge (or evidence) of meaningful consent - the legal standard applied in this project for the international transfer of personal data.

For Privacy as Expected to operate as a protocol, the conformance infrastructure for privacy records require 3 critical market conditions to scale to enable a Single Digital Market :

1. Enforceable privacy law GDPR for a single digital market (Data Sovereignty)
2. International (ISO/IEC) standard for creating a generic record of notice and consent for people
3. Internet scale (W3C) privacy vocabulary to specify a purpose with both human and machine-readable semantics.

The 2 Global Privacy Challenges:

We consider that the two global privacy challenges:

¹ EDPB, 2016, General Data Protection Regulation (GDPR)
<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>



1. Usable Access to Privacy Rights, with a Universal Privacy Signalling Protocol
2. Scaling Privacy Rights online - the implementation of a Digital Single Market on the internet requires privacy rights to scale Data Sovereignty (Privacy Agreement) infrastructure online.

These are addressed with standards, which provide an internationally neutral record format that captures a privacy notice (or surveillance sign) in a ISO standard consent record format. Which valid consent can be assessed according to a reasonable expectation of privacy. The adequacy of notice and consent as a rights measure for governance between jurisdictions can then be self-determined. In this way PasE is used to cut out the intermediaries so that data subjects can control data and consent to share personal data internationally independently of a Data Controller.

Challenges to Meaningful Consent Privacy & Rights Accessibility

'The Biggest Lie on the Internet'^{3,4}

- Lack of proof of notice for compliant consent.
- Privacy Rights information are "not automatically findable or systematically usable."
- Lack of confirmation that an Online privacy notice has been read and understood is a serious consent compliance challenge the consent receipt is designed to address.⁵
- Lack of evidence of a valid state of consent before contract terms and permissions are set with opt-ins and out's.
- Lack of usability outside of the context of the service on-boarding
- Depending on the legal justification and the parties involved, different privacy rights and obligations apply (for all parties).
 - a. When arriving on a website, consent is implied, and permissions are negotiated (not consent) and additional legal justifications applied by the Data Controller should be informed.

² Lizar, M, Binns R, 2012 "Opening up the Online Notice Infrastructure" Presented at the W3C Do Not Track and Beyond Conference .<https://www.w3.org/2012/dnt-ws/position-papers/23.pdf>

³ Lizar, 2014, Kantara Initiative [Presentation] Addressing the Biggest Lie on the Internet, with Consent and Notice Receipts, <https://kantarainitiative.org/wp-content/uploads/2014/10/Kantara-Consent-Receipt-Presentation.pdf>

⁴ Obar, 2020 The biggest lie on the internet, https://www.priv.gc.ca/en/opc-actions-and-decisions/research/funding-for-privacy-research-and-knowledge-translation/completed-contributions-program-projects/2019-2020/p_2019-20_04/

⁵ Lizar, M and Hodder, M, 2014 [Usable Consents: ConsentWorkshopSubmission-Ubicomp2014-MLizarMHodder.pdf](https://www.priv.gc.ca/en/opc-actions-and-decisions/research/funding-for-privacy-research-and-knowledge-translation/completed-contributions-program-projects/2019-2020/p_2019-20_04/)



- Data Controllers and Data Subjects have a difficult time understanding which privacy rights apply.

Data Sovereignty on the Internet

The internet originated in the USA where Terms and Conditions frameworks were invented to bootstrap a commercial Internet. They began as a one size fits all policy for online services, when digital identity and online surveillance was in its infancy. As the surveillanced evolved the policy, transparency, accountability and control didn't. The one size fits all policy framework didn't evolve, or incorporate data sovereignty safeguards, for its people, not only as 'end users' of a service.

End user license agreements, (T&Cs) and associated contract frameworks, have not implemented proportionate on reciprocal access to rights

Originally a data governance starting point, static privacy policies became a workaround forcing an op-in to terms, as a method to legitimize the surveillance permissions of online services. Referencing a privacy policy is unreasonable and not fair in a service delivery context . Today, this is a critical security flaw promoting weak Data Controller transparency with strong Data Subject surveillance. People are not often aware of who the Data Controller is or have access to privacy rights before 'opting-in' to what is mis labelled as consent. .

Extra-Territorial Considerations:

- Services based on T&Cs, for example in the USA where privacy regulation is fragmented, or in China (where the privacy law is superseded by state security) provide for a contract framework that challenge the data sovereignty of a Single Digital Market. , Obstructing access to data privacy rights which implement privacy and security people expect.
- International Trade Agreements ban data localization are also a challenge that require an international standard mechanism for people to control their own data

Providing for the economic argument for the use of a neutral internationally standardized format for the record of notice and consented as evidence of transparency . Which is why the project outputs are contributed to the Kantara Initiative's Advanced Notice & Consent Receipt (ANCR) Working Group.

Privacy as Expected : Addressing Permission Fatigue

Privacy standards are used to strengthen, simplify and improve the effectiveness of privacy rights. Standards which are adopted or enforced promise great rewards by reducing the overall costs of privacy while also increasing the overall benefits they provide. For example, Improving the trustworthiness and usability



of transparency and accountability in the use of surveillance and security systems, A, reduction in stakeholder friction and legal costs. Most importantly a better 'user' experience that facilitates access to markets, reduces the intermediary policy requirements and streamline one's own experience at a fraction of the costs.

For Usability, when privacy is not as expected, standardized and assured (witnessed) notice, notification or disclosure can be generated and independently present a corresponding Privacy notice indicator, indicating a change to the valid state of consent, like the one in this project's PaE signaling icon.

- PaE signalling is intentionally an 'at a glance' privacy measure used to contextually indicate a level of privacy assurance, centred on human expectations, to dramatically changing the paradigm in which privacy usability can be measured.
- In terms of improving human computer interaction, and relieving system permission fatigue, the PaECG protocol's works to reward practices that maintain a shared understanding of purpose and a valid state of consent.
- The receipt is used as a Measure by the Data Controller to reduce the notices and interruptions that people need to see while increasing trust in the Online interaction.

Overall, the PaECG's prototyping focus has been in the web browser in order to contrast the one-size-fits-all terms of use (contract based) model against the alternative and legally compliant personalized permission model, customised by the records Data Subject keep themselves.

2 Use-cases

A Consent Receipt is a proof of notice artifact recording a 'knowledge transaction' between the individual and one or more 'entities', similar to a conventional shopping receipt that records the exchange of money for a service or a product between the provider and the consumer. A record of the valid state. Traditionally provided using paper, receipts are now also disseminated electronically with possibilities of copies for both sellers and consumers.

A receipt, because of its inherent simplicity and familiarity as a record of a transaction to the average person, is a powerful tool for governance because:

- Consent Receipts provide proof of notice that is missing with opt-in privacy polices online, offering proof of meaningful consent, knowledge of who the controller is, and the purpose for processing and access to rights, all of which are invisible to the person online.
- Consent Receipts can be instantly generated with little preconditions or information outside of the data transaction itself.
- Consent Receipts are small, portable, contain claims, useful to port digital identifiers and easily storable.



- Consent Receipts can be self-sufficient by containing all required (meta)data concerning the transaction. In this way a functional micro-credential for rights.
- Consent Receipts are actionable artefacts, such as for asserting rights and specifying the control, storage, access, authorisation and use of personal data.
- Consent Receipts can be used to bind digital identifiers and even digital currency, and can be actionable in a truly anonymous fashion without losing its efficacy - as a bearer token.
- Critical for Privacy as Expected, Consent Receipts can be generated by the data subject, compared against each other, to see a) if the provider has posted changes (or notifications) that effect privacy for dynamic risk discovery and b) to notify of changes since the last interaction to provide proof of notice/knowledge.

Architecture

In order to support Consent Receipts, typical web and mobile applications need to provide support to a few essential mechanisms. Figure 1 illustrates our point. It is a simplified view of the wider Privacy and Data Protection. It shows four key entities. The first one, central to our project, is the user and its device. Second, it shows an online service that will collect personal information from the user.

The figure further shows two key stakeholders. A group of (generic) third parties, each a service provider (in some form) on their own, obtains personal data from the principal service provider. The second stakeholder represents the wider community, watchdogs, regulators or national authorities.

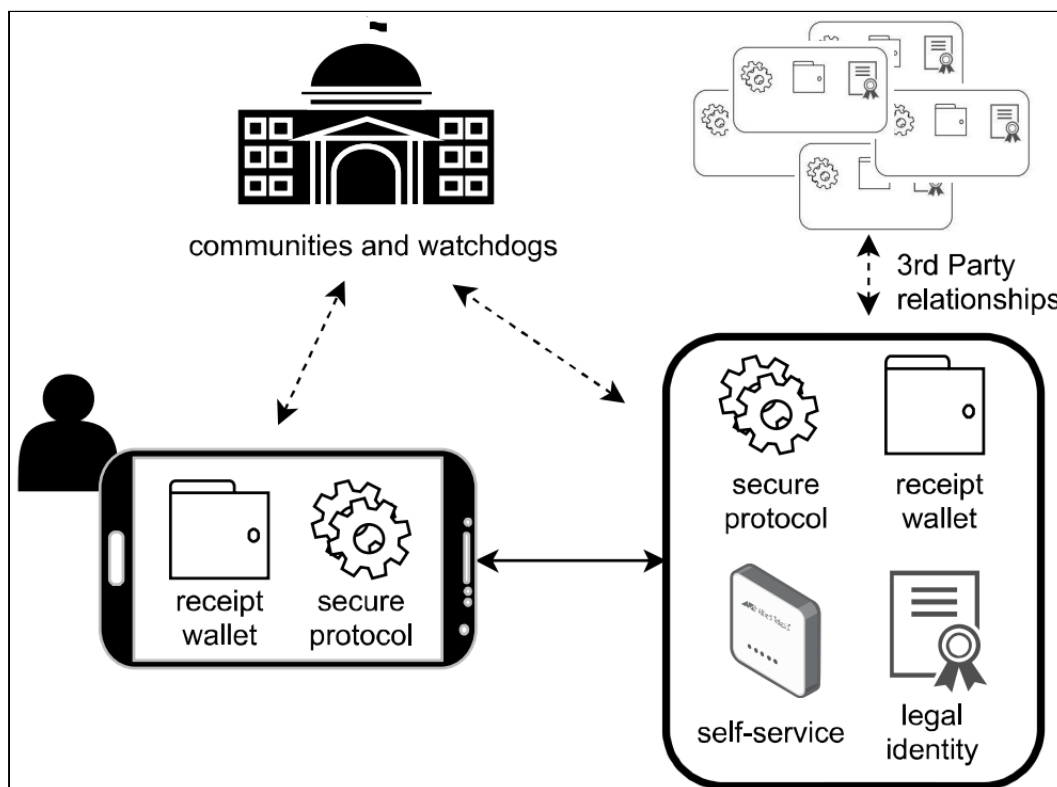


Figure 1 - Technical vision of PaECG

The data subject (aka User Agent) on the left is used to access the applications and needs two new components. First, it needs a special storage facility to generate notice records, collect, store and manage receipts. We anticipate that a single person will generate and collect many receipts per day. This component requires a User Agent such as the web browser, which is why we developed a common browser add-on extension. The extension silently generates or collects the receipts and stores them in a searchable database.

The second component on the user side is a secure protocol. As discussed before, a receipt will be of little use if one cannot trust its contents. We point to existing external work that discusses and demonstrates its implementation and feasibility (jesus_towards_2020⁶).

On the service provider side, a similar component must exist in order to run the secure protocol. It further needs its own wallet to gather receipts (potentially at scale).

Whereas the user agent does not need to present a state-accredited form of identity, the service providers must have an explicit data controller identity. In order to be compliant with laws such as GDPR and CCPA, the identity of the Data Controllers needs to be disclosed along with reaching them for access to privacy rights. For example, a form of contact must exist so that individuals can exercise their access rights, and the delivery of a receipt accomplishes this. The identity

⁶“Towards an Accountable Web of Personal Information: The Web-of-Receipts”, Vitor Jesus, IEEE Access Vol.8 <https://doi.org/10.1109/ACCESS.2020.2970270>

component of the service provider, as such, is not purely technical. It is driven from legal requirements achieved with a consent receipt that provides proof of notice.

Finally, and not necessarily a required component but rather a feature of consent receipts, we envision that service providers will offer a “self-service point” as discussed previously. Using the receipts, and not strictly needing anything else, people can independently manage their personal data with privacy rights to the extent the law allows (e.g., withdraw consent or request data deletion, object to processing, the right to be forgotten etc) to the extent the service provider is able to perform to. For example, instead of a person having to send an email to the organisation, that a human will have to manually process, people can simply use an ANCR record, to generate their (secure) receipts as a verified claim to access a control panel on the service providers website.

Use-Cases of the proof-of-Concept

We strictly followed the high-level architecture originally outlined in the proposal for the project (Fig. 1) to chart use-cases and implementat components (Fig.2):

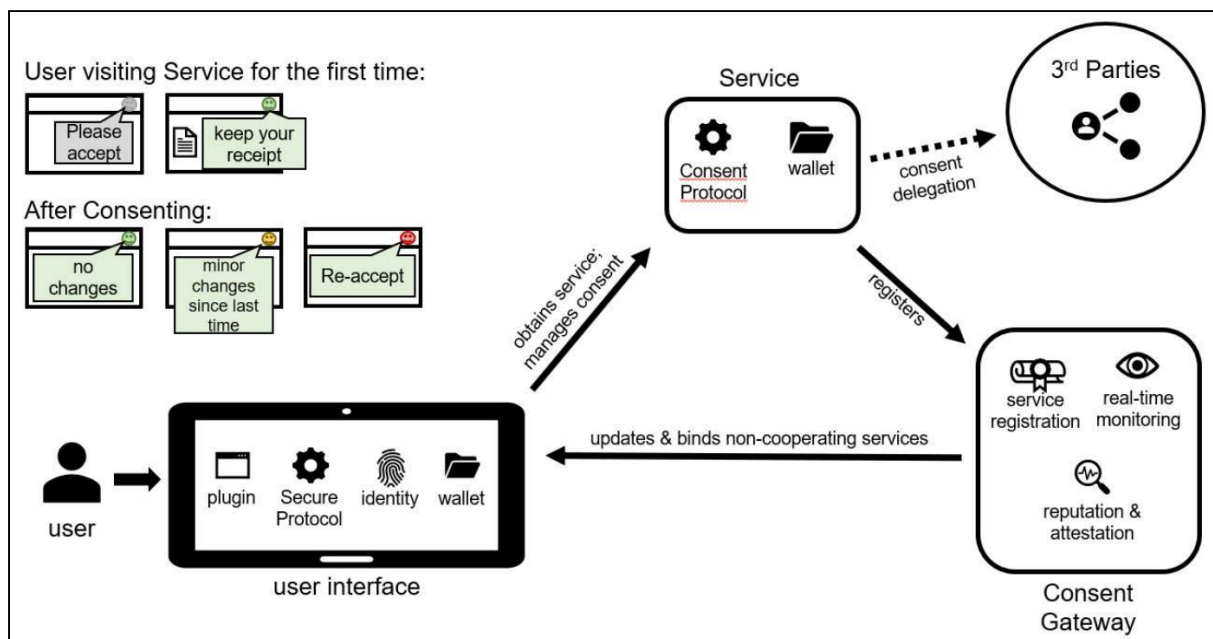


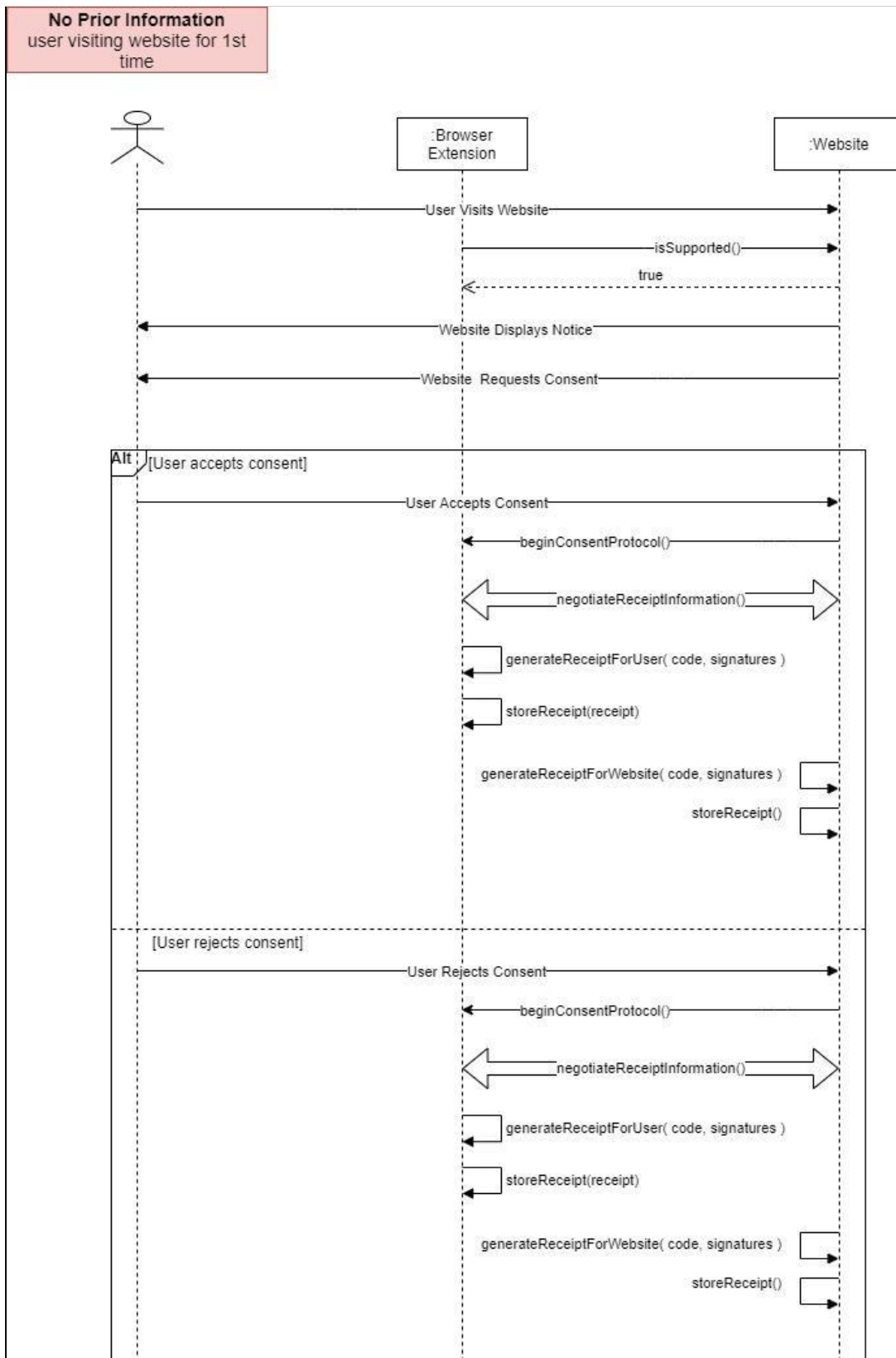
Figure 2 - Technical implementation architecture of PaECG

The PaECG project created a proof-of-concept of these relationships. We have identified the following use-cases:

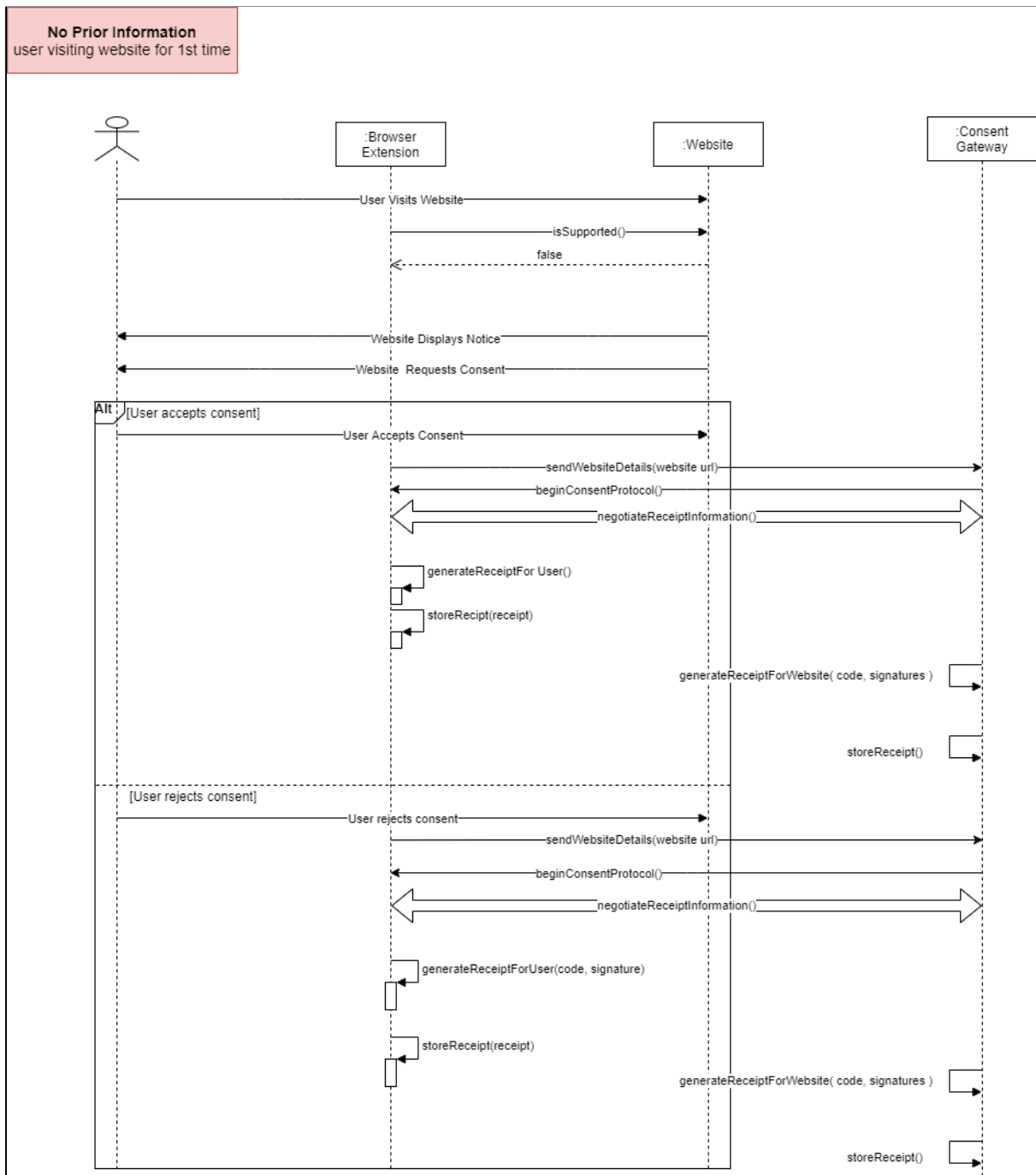
1. when the website is directly compliant with the PaECG framework
2. when the website is compliant with the PaECG framework but not directly and delegates to a Consent Gateway
3. when the website is not compliant with the PaECG framework and the user requests the engagement of the Consent Gateway
4. when third-parties collect personal information via websites

PaECG implemented the first three use-cases. Given the complexity of the fourth, we opted to leave it for future work.

The following figures show the sequence and messaging diagrams of the selected use-cases.



Use-case 1: Website directly supports the PaECG framework.



Use-case 3: Website is not compliant with PaECG so the user engages the CG on its behalf.



3 Implementation

The software implementation focused on the three key components:

- a user-agent, in the form of a browser plug-in or add-on
- a web server component
- and the accessory service of the Consent Gateway

3.1 User's Browser Extension

The user's Plug-In acts to administrate the protocol and generate the signalling protocol in order to cryptographically sign and notarize the consent notice receipt.

The first time that the plug-in is installed by the data subject, it generates a key pair that effectively creates a notional identity while being completely anonymous (if so desired). A key pair contains a private key and a public key. These keys will later be used to sign receipts and ensure their integrity. Agent Id and consent notice receipt token will be required to for proof of notice and consent and used to manage the use of receipts to make privacy rights (truly) actionable.

```
35 chrome.runtime.onInstalled.addListener(function (details) {
36     if (details.reason === "install") {
37         publicKey = keyPair.publicKey;
38         privateKey = keyPair.privateKey
39         publicKey_pem = forge.pki.publicKeyToPem(keyPair.publicKey);
40         privateKey_pem = forge.pki.privateKeyToPem(keyPair.privateKey);
41         userId = createUUID();
42         userToken = generateToken(16);
43
44         let config = {
45             'userId': userId,
46             'privateKey': privateKey_pem,
47             'publicKey': publicKey_pem,
48             'userToken': userToken,
49         };
50         saveToLocalStorage('config', config);
51         chrome.tabs.create({
52             url: "/popup/config.html"
53         });
54     }
55 });
```

After the PaE plug-in is installed in the browser it opens a page to show the configuration to the user. The configuration file contains the key pair, the record log, the user id and the token for the user. The user can save the configuration file for future use. It is advised to download the record log stored in the file to a safe/secure place and import receipt store on a new device to access privacy rights and for future uses (e.g. service/product discovery).

Userld

Token

PrivateKey

PublicKey

[Download Config File](#)

When a user visits a website, the browser plug-in checks if the website supports the protocol or not. The website must explicitly mention it supports the protocol. The website needs to add additional metadata to the website to inform the plug-in it supports the protocol.

```
5 <meta name="pisp" content="ws://3.10.208.186:3100">  
6 <meta name="lastPolicyUpdateDate" content="2020-12-20">
```

Also, the website should include additional `paecg.js` file so the website and the plug-in can communicate with each other.

```
69 <script src="paecg.js"> </script>
```

If the website wants to be compliant with the protocol, then information about the consent submission elements, user inputs fields, JavaScript being used in the page and link to the policy URL should be provided in the correct format. Additional information about the data controller can be also mentioned.

How to provide configuration information to the plug-in.

1. Add the `paecg.js` file to the page.



2. Create a new instance of PaECG with correct JSON fields and format.
3. Call setup method on PaECG instance created on step 2.

JSON fields and format to be provided are as follows:

- info_for_receipt= required, JSON, is used to give additional information about the data controller and data, can be left blank if the user does not want to give additional information.
- consent_submission_elements= required, JSON, is used to provide information about elements responsible for handling the consent interaction.
- user_inputs= required Array, is used to provide information on elements having the user data.
- javascript= required Array, is used to give information on the JavaScript files included in the page.
- policyurl= required Array, is used to give information on the privacy policy page linked to the page.


Example

```
70 <script>
71 var details={
72   'info_for_receipt':{   'piicontrollers':[{
73     "name": "Acme Inc.",
74     "localid": "PIIC-A",
75     "address": "Wonderland",
76     "url": "http://example.com/",
77     "contact": {
78       "phone": "000",
79       "email": "acme@example.com"
80     },
81     "policies": {
82       "privacy": "http://example.com/privacy",
83       "termsconditions": "http://example.com/tandc"
84     }
85   }]},
86   'consent_submission_elements':{'Submit':'Accept'},
87   'user_inputs':['fname','lname','email'],
88   'javascript':['http://3.10.208.186/js/one.js','http://3.10.208.186/js/two.js'],
89   'policyurl':['http://3.10.208.186/policy/one.html','http://3.10.208.186/policy/two.html']
90 };
91 var paecg=new PaECG(details);
92 paecg.setup();
93 </script>
```

The plug-in checks if the website supports the protocol and displays it to the user.

```
40 function isSupportedWebsite() {
41   return (($("meta[name='pisp']").length > 0);
42 }
```




Not Supported Privacy as Expected : Consent Gateway 

Generate Receipt

Show all receipts Current Site Receipts

No receipts found for this site

Supported Privacy as Expected : Consent Gateway 

Last policy change date: 2020-12-20

Since last agreement, no changes have been made

You clicked on Accept last time on Fri Mar 26 2021 15:19:17 GMT+0000 (Greenwich Mean Time)

Show all receipts Current Site Receipts

When there is consent interaction between a user and a website on a PaECC compliant website then a message is sent to the Plug-in's Content Script.



```
50     runProtocol(element) {
51         var PII = {}
52         for (var thisInput of this.user_inputs) {
53             PII[thisInput] = document.getElementById(thisInput).value;
54         }
55         var user_click=this.consent_submission_elements[element];
56         var clicked_element=JSON.stringify(document.getElementById(element).outerHTML);
57         window.postMessage({
58             type: "FROM_PAGE",
59             title: 'fetchConsentDetails',
60             PII: PII,
61             clickedElement:clicked_element,
62             user_click_value:user_click,
63             thirdparties: this.thirdparties,
64             javascriptUrls:this.javascript,
65             policyUrls: this.policyurl,
66             all_receipt_data:this.all_receipt_data
67         }, "");
68         console.log('Sending click response ...');
69     }
70 }
```

The Content Script listens to the event and retrieves all the information from the webpage and starts the protocol.

```
565 window.addEventListener("message", function (event) {
566     if (event.source != window)
567         return;
568     if (event.data.type && (event.data.type == "FROM_PAGE")) {
569         switch (event.data.title) {
570             case "fetchConsentDetails":
571                 /**Get all Info */
572                 clickedElement = event.data.clicked_element;
573                 PII = event.data.PII;
574                 consentText = event.data.user_click_value;
575                 allJavascriptUrls = event.data.javascriptUrls;
576                 allPolicyLinks = event.data.policyUrls;
577                 consent_data = event.data.consent_data;
578                 info_for_receipt = event.data.info_for_receipt;
579                 /* Run the Protocol*/
580                 generateReceiptForCompliant();
581             }
582         }
583     });
```

The protocol generates a current timestamp as the timestamp of the interaction between the user and the website. Then it gets all the Java Scripts, Policy pages



from the URLs provided by the website. It also gets the HTML of the page. After gathering all the files, it hashes them.

```
241 | timestamp=new Date().getTime();
242 | console.log('Generate Receipt For Compliant');
243 | /* Run the Protocol*/
244 | Promise.all([gatherJavascriptFiles(allJavascriptUrls),
245 | gatherPolicyFiles(allPolicyLinks), getHtml()]).then(() => {
246 |     hashContents().then(() => {
```

If the website is compliant with its own receipt generator, then it will create a WebSocket connection with the website's receipt generator. But if the website does not have receipt generator, then it will create a WebSocket connection with the consent gateway.

```
248 | | | if (pispUrl == 'Consent Gateway') {
249 | | |     pispUrl = 'ws://46.101.26.188';
250 | | | }
```

The user Plug-In sends a message to the WebSocket with all the URLs provided by the website.

```
let messageToSend = {
  title: "getContentAndHash",
  data: {
    info_for_receipt: info_for_receipt,
    consentText: consentText,
    clickedElement: clickedElement,
    javascriptUrls: allJavascriptUrls,
    policyUrls: allPolicyLinks,
    htmlUrl: window.location.href,
  },
};
```



If the website is using the consent gateway, a consent receipt is generated that uses the information as above and requests verification with signatures.

```
267 |     websocket.send(JSON.stringify(messageToSend));
```

When the receipt generator gets the message, it starts to hash the contents. When the hashing is completed by the receipt generator then it sends all the hashes back to the plug-in.

```
270 |     websocket.addEventListener("message", message => {  
271 |         let message_data = JSON.parse(message.data);  
273 |         if (message_data.title == "hashingCompleted") {
```

The user Plug-in checks if the hashes generated by the plug-in and receipts generator are the same. As both the plug-in and server component are fetching the contents from the URL independently, the contents should be the same, and therefore the hashes must be the same, if both are honest. When hashing is completed the plug-in sends a message to the receipt generator to start the signing process along with the data involved. The Plug-in also starts to sign the details on its end. When the signing is completed, signed messages are exchanged between both ends.

```
278 |         let sendPII = { 'title': 'getSignedMessage', 'data': { PII } };  
279 |         websocket.send(JSON.stringify(sendPII));  
  
284 |         sendMessageToBackground('signDetails', messagetoSign);  
  
291 |         if (verify_signed_message(message_data)) {
```

If the signed message received from the receipt generator is valid then the plug-in starts to create a JSON file using the details gathered. Then the JSON is saved to the cloud. Users can also save the file locally into the device.

```
335 |         sendMessageToBackground("saveToCloud", cloudReceiptData)  
337 |         downloadReceipt(JSON.stringify(receipt_structure), `receipt_${receiptId}`);
```

All the receipts previously generated are displayed to the user in the plug-in. The Plug-in can filter receipts according to the website being visited. Plug-in allows users to download the receipt from the plug-in.

The screenshot shows a user interface for a privacy consent gateway. At the top left, there is a green pill-shaped button labeled 'Supported'. To its right, the text reads 'Privacy as Expected : Consent Gateway' and 'Last policy change date: 2020-12-20'. A blue gear icon is in the top right corner. Below this, a light green box contains the text 'Since last agreement, no changes have been made'. A grey box below that shows 'You clicked on Accept last time on Fri Mar 26 2021 15:19:17 GMT+0000 (Greenwich Mean Time)'. Two buttons, 'Show all receipts' and 'Current Site Receipts', are positioned below. At the bottom, there are two identical icons: a document with a download arrow and an eye icon.

The User plug-in also works for PaECG non-compliant websites as well. A user willing to generate a receipt on PaECG non-compliant website has to click on the 'generate receipt' button in the plug-in before doing any consent interaction on the website.

The screenshot shows a user interface for a privacy consent gateway that is not supported. At the top left, there is a red pill-shaped button labeled 'Not Supported'. To its right, the text reads 'Privacy as Expected : Consent Gateway'. A blue gear icon is in the top right corner. Below this, a dark grey button labeled 'Generate Receipt' is visible. Two buttons, 'Show all receipts' and 'Current Site Receipts', are positioned below. At the bottom, the text reads 'No receipts found for this site'.

When there is any interaction on the web page then the plug-in collects all the JavaScript URLs used in the page, it also tries to gather all the privacy policy links in the page.



```
432     consentText = element.value;
433     allJavascriptUrls = [];
435     Array.prototype.slice.call(document.scripts).forEach(element => {
436         if (element.src != "") {
437             allJavascriptUrls.push(element.src);
438         }
439     });
```

After gathering all the links from the page, the plug-in fetches all the javascript files, policy pages. The Plugin also gets all the data from the input fields in the page. After getting the required data, the plug-in hashes all the contents.

```
442     Promise.all([gatherJavascriptFiles(allJavascriptUrls),
443                 getAllPrivacyPolicyUrls(), gatherPolicyFiles(allPolicyLinks), gatherAllPII(),
444                 getHtml()]).then(() => {
445         hashContents().then(() => {
```

Then the plug-in creates a connection with the consent gateway. The Plug-in sends all the links to the consent gateway. The Consent gateway gets all the files from the links and sends the hashes of them back to the plug-in. The Plug-in checks if the hashes are matching. If the hashes are the same, then the plug-in sends a message to the consent gateway to start signing the details. The plug-in also starts to sign the details. After receiving the signed message from the consent gateway, the Plug-in checks if the signed message is valid. If the signature is valid then the plug-in makes a file from the details gathered previously. The Plug-in saves the generated receipt to the cloud and prompts the user to save the receipt locally as well. The Plug-in also sends the signed message to the consent gateway when it finishes signing the details.

3.2 Web Server Module

The web server Component is responsible for handling the requests from the user plug-in.

For this project, Node.js with express JS is used in the backend to handle the requests from the plug-in. But any language and any frameworks can be used to configure the web server component.

The Web Server component communicates with the plug-in using a WebSocket to generate receipts. The server component is also referred to as receipt generator. The web server component requires a key pair. These keys will be used when exchanging and verifying the consent details.



```
9   const wss = new WebSocket.Server({
10  |     port: 3100
11  | });

23  const rsa = forge.pki.rsa;
24  const keyPair = rsa.generateKeyPair({
25  |     bits: 1024,
26  |     e: 0x10001
27  | });
28  const publicKey = keyPair.publicKey;
29  const privateKey = keyPair.privateKey
30  const publicKey_pem = forge.pki.publicKeyToPem(keyPair.publicKey);
31  const privateKey_pem = forge.pki.privateKeyToPem(keyPair.privateKey);
```

It 'listens' to the connections from the plug-in.

```
34  wss.on("connection", ws => {
36  |     ws.on("message", data=>{
```

When there is a connection from the plug-in, the WebSocket retrieves data as JSON. The Plug-in sends data to the server component in the specific format for different purposes. This JSON has a title field to instruct the server component which action to perform on retrieving the message. The data field contains all the data to facilitate the action to be performed.

```
37  |     |     let message=JSON.parse(data);
```

The different actions that request that the Web Server component can receive, and how to respond to those requests, are mentioned below.

On receiving the title "getContentsAndHash" from the browser addon, Web Server component has to hash all the contents such as HTML, Privacy policy pages, and JavaScript pages. It has to send the hashes back to the Plug-in in a specified format.

Message from the Plug-in.

- "title": getContentsAndHash
- "data": JSON
 - "javascriptUrls", Array, Javascripts links in the page
 - "policyUrls", Array, of all the policy pages links in the page.



- “htmlUrl”, String, URL of the page.
- “consentText “, String, Consent Text of the Interaction
- “info_for_receipt” JSON, Additional Information

Format to send message back:

- “title”: 'hashingCompleted', Required.
- “data”: JSON, Required.
 - “javascriptHash”, Required, String, JavaScript hash of all the JavaScript pages combined.
 - “policyHash”, Required, String, Hash of all the policy pages combined.
 - “htmlHash”, Required, String, Hash of the HTML of the page.

When receiving “getContentsAndHash” as a message title from the Plug-in, the Web Server Component gets all the necessary information such as HTML, Privacy policy pages, and JavaScript links. It iterates through all the links, fetch contents of all the links and hashes them.

```
47 | | Promise.all([gatherPolicyFiles(),
48 | | gatherJavascriptFiles(),
49 | | getHtml()]).then(() => {
50 | | generateHash().then(() => {

130 | async function getHtml(){
131 | |   htmlContent=await getContentFromUrl(htmlUrl);
132 | | }
133 |
134 | async function gatherJavascriptFiles() {
135 | |   allJavascriptContent='';
136 | |   for (let javascripturl of javascriptUrls) {
137 | | |   let javascriptcode = await getContentFromUrl(javascripturl);
138 | | |   allJavascriptContent += javascriptcode;
139 | | | }
140 | | }
141 |
142 | async function gatherPolicyFiles() {
143 | |   allPolicyContent='';
144 | |   for (let policyUrl of policyUrls) {
145 | | |   let policyUrlContent = await getContentFromUrl(policyUrl);
146 | | |   allPolicyContent += policyUrlContent;
147 | | | }
148 | | }
```

Another request that the web server component can receive, is to sign the details involved in the consent interaction. When the Plug-in gets the message with the title “getSignedMessage”, it should start to sign the details and send the signed details back.

Message from the user Plug-in.

- “title”: “getSignedMessage”
- “data”: JSON
 - “PII”, JSON, User data used in the consent interaction.

```
58 if (message.title == "signedMessage") {
59   let user_public_key = forge.pki.publicKeyFromPem(message_data.public_key);
60   let user_signed_message = message_data.signed_Data;
61   let consent_details={
62     htmlContent: htmlContent, javascript: allJavascriptContent,
63     policy: allPolicyContent, PII: message_data.PII,
64     timestamp: message_data.timestamp, nonce: message_data.nonce,
65     info_for_receipt
66   };
67   let messageDigest = forge.md.sha256.create();
68   messageDigest.update(consent_details, 'utf8');
69   let verify = user_public_key.verify(messageDigest.digest().bytes(), user_signed_message);
```

The message to send back to the Plug-in is shown below.

- “title”: “signedMessage”, Required.
- “data”: JSON, Required.
 - “signedMessage”, Required, String, JavaScript hash of all the JavaScript pages combined.
 - “server_publickeypem”, Required, String, Hash of all the policy pages combined.
 - “timestamp”, Required, Number (Javascript), Hash of the HTML of the page.
 - “nonce”, Required,String Nonce.

The signed message also needs to be in the correct format. The Web Server component signs the JSON data with specific field and data. The JSON and fields are explained below.

- htmlContent: HTML page of page.
- javascript: Content of all the JavaScript used in the page.
- policy: Content of all the policy pages used in the page.
- PII: User data used in the consent interaction.



- timestamp:timestamp
- nonce:nonce
- info_for_receipt: additional information about the page.

```
99     if(message.title=='getSignedMessage'){
100         let timestamp=new Date().getTime();
101         let nonce=( 1e9*Math.random()*1e9*Math.random() ).toString(16);
102         let consent_details={
103             htmlContent: htmlContent, javascript: allJavascriptContent,
104             policy: allPolicyContent, PII: message_data.PII, timestamp: timestamp,
105             nonce: nonce, info_for_receipt: info_for_receipt
106         };
107         let rc = forge.md.sha256.create();
108         rc.update(consent_details, 'utf8');
109         let signedMessage = privateKey.sign(rc);
110         console.log("Data Signed By the Server")
111         let data = {
112             signedMessage: signedMessage,
113             server_publickeypem: publicKey_pem,
114             timestamp:timestamp,
115             nonce:nonce
116         };
117         console.log("Sending Signed Data To the Client");
118         ws.send(JSON.stringify({'title':'signedMessage','data':data}));
119     }
120 }
```

In the case where the Web server component receives a message with the title “signedMessage” it verifies if the signature is valid. If the signature is valid then it gathers all the previous information and generates a JSON file as the receipt and saves it locally.

Message from the user Plug-in.

- “title”: “signedMessage”
- “data”: JSON
 - “public_key”, public_key of the user plug-in. Public key is in PEM format.
 - “signed_Data”, the data user plug-in signed.

As all the hashes matched previously, all the contents must be the same at both ends. The Web component gathers all the information and makes a JSON in the same format that the Plug-in signed it. The Web component checks if the signed



message from the Plug-in is authentic and has not been tampered with. When the web server component verifies the signed message, it creates and saves a JSON file with all the details gathered previously.

```
73     let receiptData = {
74         'identifier': message_data.receiptId,
75     };
76     receiptData['paecg']={
77         'user_public_key':message_data.public_key,
78         'signed_Messaged': message_data.signed_Data,
79         'DataSigned':consent_details,
80         'PII':message_data.PII,
81         'html':htmlContent,
82         'javascript':allJavascriptContent,
83         'policy':allPolicyContent,
84         htmlHash,javascriptHash,policyHash
85     }
86     let fileName=`receipts/receipt${message_data.receiptId}.json`;
87     fs.writeFileSync(fileName, JSON.stringify(receiptData));
88     console.log("Receipt Downloaded successfully.....");
```

3.3 Consent Gateway

The PaE Protocol, facilitated by Consent Gateway is designed to produce a proof of privacy notice record, for the semantically standardized [W3C vocabulary](#), utilising the ISO/IEC 29100 Privacy framework for baseline term definitions for stakeholders. This is further elaborated on in the ISO/IEC 29184 Online privacy notices and consent standard, in which an example of the Consent Receipt is published in the appendix, and further developed in ISO/IEC 27560.3 (WD3) Consent Record information structure.

The Consent Gateway's function is to aid in the verification and non-repudiation of the state of consent and permissions, captured in the Consent Receipts when the Data Controller does not directly provide proof with a Consent Receipt. It addresses the gap where people tick boxes asserting that they read a policy that they then can't track.

How the Consent Gateway is operated

When the Website does not have the capacity to generate a receipt, the user Plugin can generate a record and send it to the Consent Gateway to sign the record and generate the receipt. The Consent Gateway acts as a witness to the notice between the website and the user.

The user Plug-in communicates with the Consent Gateway to generate receipts. It is similar with the web server component part, where the WebSocket is used as secure way to communicate between the endpoints.

When the Consent Gateway receives a message from the user Plug-in, firstly it verifies the controller and website information provided by the user's (data subject's) Plug-in. It generates a mirrored record from this verification and stores it in the Consent Gateway Ledger as a proof of notice.

Then it checks if the request is for a compliant or non-compliant website and handles the request accordingly.

If the request is to hash contents for the complaint website, it sends hashes back to the Plug-in after fetching all content of all the required URLs.

```
90     if (
91         message.title == "getContentsAndHash" &&
92         message.website_type == "compliant"
93     ) {
103         Promise.all([getHtml(htmlUrl),
104             gatherJavascriptFiles(javascriptUrls),
105             gatherPolicyFiles(allpolicyUrls),
106         ]).then(() => {
107             generateHashcompliant().then(() => {
```

If the request is from a non-compliant notice information on the website, then Consent Gateway captures the html and the privacy and terms policy alone, together with the URL's, JavaScript and the contents of the policies, before hashing them and sending them back to the user Plug-in. The plug-in then sends the data as a record (using the PaE protocol and format) to the Consent Gateway to sign the record to turn it into the Consent Receipt (a type of verified claim).



```
200     if (message.title == "getSignedMessage") {
201         let timestamp = new Date().getTime();
202         let nonce = (1e9 * Math.random() * 1e9 * Math.random()).toString(16);
203         let consent_details = {
204             htmlContent: htmlContent,
205             javascript: allJavascriptContent,
206             policy: allPolicyContent,
207             PII: message_data.PII,
208             timestamp: timestamp,
209             nonce: nonce,
210         };
211
212         let rc = forge.md.sha256.create();
213         rc.update(consent_details, "utf8");
214         let signedMessage = privateKey.sign(rc);
215         console.log(">>>>>Data Signed By the Server<<<<<<<");
216         let data = {
217             signedMessage: signedMessage,
218             server_publickeypem: publicKey_pem,
219             timestamp: timestamp,
220             nonce: nonce,
221         };
222         console.log("Sending Signed Data To the Client");
223         ws.send(
224             | JSON.stringify({ title: "signedMessageFromConsentGateway", data: data })
225         );
226     }
```

When the user's (Data Subject's) browser Plugin sends the record to the Consent Gateway with a title "signed message" it verifies the website information captured in the record. If the captured information is validated then the Consent Gateway generates a Consent Receipt JSON file with all the information previously gathered as the proofs' payload. The receipt is saved in the ledger linked to the Consent Gateway server. If the data controller information or the signature is not valid then the consent gateway discards the record and does not generate the receipt.



```
121 | if (message.title == "signedMessage") {
122 |   console.log(message.data);
123 |   let user_public_key = forge.pki.publicKeyFromPem(message_data.public_key);
124 |   let user_signed_message = message_data.signed_Data;
125 |   let consent_details={
126 |     htmlContent: htmlContent, javascript: allJavascriptContent, policy: allPolicyContent,
127 |     PII: message_data.PII, timestamp: message_data.timestamp, nonce: message_data.nonce, info_for_receipt
128 |   };
129 |   console.log("Signed Message From Client");
130 |   let messageDigest = forge.md.sha256.create();
131 |   messageDigest.update(consent_details, 'utf8');
132 |   let verify = user_public_key.verify(messageDigest.digest().bytes(), user_signed_message);
133 |   // If the signature is valid then
134 |   if (verify) {
135 |     console.log("Signature is Valid");
136 |     let receiptData = {
137 |       'identifier': message_data.receiptId,
138 |     };
139 |     receiptData['paecg']={
140 |       'user_public_key':message_data.public_key,
141 |       'signed_Messaged': message_data.signed_Data,
142 |       'DataSigned':consent_details,
143 |       'PII':message_data.PII,
144 |       'html':htmlContent,
145 |       'javascript':allJavascriptContent,
146 |       'policy':allPolicyContent,
147 |       htmlHash,javascriptHash,policyHash
148 |     }
149 |     let fileName=`receipts/receipt${message_data.receiptId}.json`;
150 |     fs.writeFileSync(fileName, JSON.stringify(receiptData));
151 |     console.log("Receipt Downloaded successfully.....");
152 |   }
153 |   else{
154 |     console.log('Signature not valid from client');
```

3.4 Consent Receipts

This section provides a summary of the work conducted regarding Consent Receipts in terms of exploring information required for assessing and demonstrating the ‘validity of consent’ according to specific legal requirements. The data set required to be recorded regarding consent and its provision is dictated by legal requirements and is provisioned as a Consent Receipt for providing verifiable and accountable records to involved stakeholders. The data required, the specification and format into which it is put, and its relation to GDPR is explored in more detail within the ‘Deliverable 2.4 Consent Receipt’ and is published at the PaE:CG website⁷ as well as deposited to Zenodo⁸ for long-term availability and archival.

The public Consent Receipt (v1.1) was published by Kantara Initiative in 2018. This version is not compatible with the current laws, their interpretations, and the ecosystem within which they operate, more specifically regarding the changes following GDPR’s enforcement in 2018. This is primarily due to the consent receipt specification utilising different terminology and the difference in information from what is required as per GDPR’s requirements for consent. The primary aim

⁷ <https://privacy-as-expected.org/deliverables.html>

⁸ <https://doi.org/10.5281/zenodo.5076603>



of this work is therefore to provide a Consent Receipt specification based on GDPR's requirements regarding consent.

Additionally, the work also provided an exploration of the following objectives:

1. Providing trust, transparency, and accountability by utilising cryptographic signatures - as explored in prior work⁹
2. Operating within a global landscape consisting of multiple non-compatible jurisdictions - and the role of standards such as ISO/IEC 29100¹⁰ and 29184¹¹ in assessing adequacy while harmonising vocabulary and application
3. Specifying information required within the receipt in online notices and the webpages they operate within.

Within the PaE:CG project, the deliverable D2.4 Consent Receipt guides the information fields utilised by the other deliverables, which are: D2.1 User Plug-in, D2.2 Consent Gateway, and D2.3 Server Component. While the implementations of these latter deliverables use only a *subset* of the possible fields, the D2.4 deliverable outlines the superset of fields possible for inclusion and their role within the consent processes.

The identification of relevant information is based on analysis of currently enforced European data protection and privacy laws, including ePrivacy Directive (ePD, 2002) and the General Data Protection Regulation (GDPR, 2016). The laws provide the basis for information necessary to be provided to individuals - both within the context of consent as well as for other purposes associated with the processing of personal data, and the consideration of 'validity of consent' based on meeting certain requirements. These requirements were interpreted to record specific 'fields of information' that can be used to demonstrate or verify the authenticity and legitimacy of consent obtained or given, as well as other interactions within the context such as the provision of notice, information about rights, or the proposed processing of personal data dependent on that consent.

Given that the Consent Receipt (v1.1, 2018) is an existing specification, the PaE:CG project first assessed the capability and extent of it meeting the requirements for specifying the required information. Based on this, necessary changes were identified and codified into the newer set of fields intended to be recorded within a receipt. Both the analysis and the fields are presented within the more comprehensive D2.4 deliverable. Additionally, requirements were also obtained from the ISO/IEC 29184 Online privacy notices and consent given its important role in the standardisation of the process and information in scope for the PaE:CG project.

A list of possible fields based on interpreting the above information is presented in the table below. The list consists of questions involved in assessing the validity of consent, and the required 'concept of information' necessary to answer or evaluate the requirements based on that question.

⁹ Jesus, V. (2020). Towards an Accountable Web of Personal Information: The Web-of-Receipts. IEEE Access, 8, 25383–25394. <https://doi.org/10/ggsgh4>

¹⁰ <https://www.iso.org/standard/45123.html>

¹¹ <https://www.iso.org/standard/70331.html>



Questions about Receipt	Fields
How to uniquely identify or reference this receipt?	Receipt ID
How to uniquely identify or reference the schema of this receipt?	Receipt Schema
When was this receipt generated?	Receipt Generation
Who generated this receipt?	Receipt Generating Entity
How was this receipt generated?	Receipt Generation Method
Why was this receipt generated?	Receipt Generation Timestamp
What location was this receipt generated and provided at?	Receipt Provision Location
What medium was this receipt generated and provided in?	Receipt Provision Medium
What is the language of information used by this receipt?	Receipt Language
What is the encoding of information used by this receipt?	Receipt Encoding
Is the receipt signed?	Receipt Signatures
Who has signed this receipt?	Receipt Signing Entity
What is the role of each entity that has signed this receipt?	Receipt Signing Entity Role
What is the algorithm used in the signature?	Receipt Signing Algorithm
What is the value of the signature?	Receipt Signature
What is the checksum of receipt for verification of integrity?	Receipt Checksum
What is the format of the checksum?	Receipt Checksum Format
Does this receipt replace or void another receipt?	Receipts Replaced
Is this receipt a companion to another receipt?	Relevant Receipts
Questions about Entity	
What is the (legal) name of this entity?	Entity Legal Name
What is the type of this entity?	Entity Legal Type
What is the legal (identifier) of this entity?	Entity Legal Identifier
What is the URL of this entity?	Entity URL
What is the physical address of this entity?	Entity Physical Address
What is the communication point for contacting this entity?	Entity Communication Point
What is the type of contact for this entity?	Communication Type
What is the value of contact for this entity?	Communication Details
What are the relevant policies for this entity?	Entity Policies
What is the URI for the policy for this entity?	Policy URI
What is the type of policy for this entity?	Policy Type
What is the version for the policy for this entity?	Policy Version
What is the checksum for this policy?	Policy Checksum
What is the public key for this entity?	Entity Public Key
What is the algorithm or type for the cryptographic public key for this entity?	Public Key Algorithm
Questions about Notice containing Consent Request	



Who provided the notice?	Notice Providing Entity
What is the identifier or URL for the notice?	Notice ID
What is the version of the notice?	Notice Version
What is the timestamp of the notice?	Notice Timestamp
What is the method used for providing the notice?	Notice Provision Method
What is the location used for providing the notice?	Notice Provision Location
What is the medium used for providing the notice?	Notice Provision Medium
What is the form of the notice?	Notice Form
What is the language used for providing the notice?	Notice Language
What is the checksum of the notice?	Notice Checksum
Was the notice associated with consent or matters other than those presented in the receipt?	Notice Provision Purposes
What information about personal data and its processing was provided?	Notice for Personal Data Processing
Questions about Choice regarding Consent	
What choices were presented in the notice?	Choices
What was the type of impact for the choice presented?	Choice Type
What was the value of label for the choice presented?	Choice Label
What was the method for indicating the choice?	Choice Indication Method
Was this the choice chosen?	Choice Indication
When was the choice chosen?	Choice Indication Timestamp
What is the location used for providing the choice?	Choice Provision Location
What is the medium used for providing the choice?	Choice Provision Medium
What is the language used for providing the choice?	Choice Provision Language
What is the form of the choice?	Choice Form
Who made this choice?	Choice Made By Entity
What is the relationship of the Entity that made the choice with the data subject?	Entity Relationship with Data Subject
Is there an expiry or validity duration for this choice?	Choice Validity / Duration
Is there a condition or event that invalidates this choice?	Choice Invalidation Conditions
How can this choice be changed or discarded?	Method for Changing Choice
Questions about Consent	
What is the consent decision recorded in the receipt?	Consent Decision
What is the status of consent?	Consent Status
What is the type of consent?	Consent Type
What is the label used to indicate consent?	Consent Indication Label
What is the method used to indicate consent?	Consent Indication Method
What is the timestamp for decision regarding consent?	Consent Timestamp



What is the location where decision regarding consent was made?	Consent Location
What is the medium where decision regarding consent was indicated?	Consent Medium
Who made the decision regarding consent?	Consent indicated by Entity
What was the relationship of decision making entity to individual?	Entity Relationship to Data Subject
When does this decision regarding consent expire or what is its duration?	Consent Duration
What are the conditions under which this decision regarding consent is no longer valid?	Consent Invalidation Conditions
How to change decision for consent or to withdraw it?	Method for Changing Consent or Consent Withdrawal
Questions about Jurisdiction and Legality	
What are the jurisdictions applicable for this record?	Jurisdiction
What are the types of applicable jurisdictions for this record?	Jurisdiction Type
What are the authorities relevant for this record?	Authority
What are the rights included or provided based on jurisdictions for this record?	Rights
Who exercises the right?	Right exercised by
How to exercise the right?	Method for Exercising Right
What is the form of information required for exercising the right?	Information Required for Rights
Questions about Personal Data Handling	
What are the purposes for which consent is required?	Purpose
What is the type or category of Purpose?	Purpose Category
What is the value or label used for Purpose?	Purpose Label
Who is responsible for the Purpose?	Responsible Entity for Purpose
What Personal Data or Personal Data Categories are required for this purpose?	Personal Data (/Categories)
Is the personal data of sensitive or of special categories?	Sensitive or Special Category Personal Data
Is the personal data of identifying nature or is an identifier?	Identifier or Identifying Personal Data
Is the personal data inferred or derived?	Inferred / Derived Personal Data
How is the personal data collected?	Data Collection Method
Where is the personal data collected from?	Data Collection Source
What is the frequency of Personal Data collection?	Data Collection Frequency
What is the duration over which Personal Data will be collected?	Data Collection Duration
Are any processors involved in personal data collection?	Processors
How is personal data stored?	Data Storage Method
Where is the personal data stored?	Data Storage Location
How long is personal data stored for?	Data Storage Duration



What happens after data storage period expires?	Data Deletion Policy
Is data securely stored?	Data Storage, Security
Are any processors involved in personal data collection?	Processors, Data Storage Collection
What (other than collect, store, and delete) processing operations required for purpose?	Processing Activity
Who is responsible for carrying out the processing operation?	Processor
Where will the processing be carried out?	Processing Location
Will the Personal Data be shared with other recipients?	Recipients, Data Sharing
Who will be sharing the Personal Data?	Data Sharing Entity
Who will be receiving the shared Personal Data?	Recipient
What will be the frequency of sharing Personal Data?	Data Sharing Frequency
What will be the method of sharing Personal Data?	Data Sharing Method
What will be security measures involved in sharing of Personal Data?	Data Sharing, Security
Questions about Risks and Risk Management	
At any point, will the personal data move outside the stipulated jurisdictions?	Jurisdiction, Data Transfer
If personal data is moved outside stipulated jurisdiction, what are the justifications?	Jurisdictions
Does the purpose involve any automated decision making?	Automated Decision Making
Does the purpose involve processing at large scales?	Large Scale Processing
Does the purpose involve monitoring or profiling of the individual(s)?	Monitoring, Profiling
Does the purpose involve any novel or uncertain use of technologies?	Novel, Uncertain Technologies
Does the purpose involve creation of scores or measures of the individual(s)?	Scores, Measurements
What risks are involved in the processing of personal data?	Risks
What is the likelihood of risk to happen?	Risk Likelihood
What is the severity of impact if risk does happen?	Risk Severity
What are the mitigation measures undertaken to prevent and address the risk?	Risk Mitigation Measure
What are the technical measures undertaken to safeguard the data and privacy?	Technical Measures
What are the organisational measures undertaken to safeguard the data and privacy?	Organisational Measures
Questions about Standards, Signals, Measures related to Consent/DataProtection/Privacy	
Are there any specific standards, signals, or measures indicated by the individual or their agent in connection with this record?	Signals, Standards, Measures
What is the method for providing the signal or measure?	Signal Method
What is the value of the signal or measure?	Signal Value

This information can be specified in the form of machine-readable (meta-)data by using the following methods:

1. As JSON or JSON-LD data structures ready for use in a wide range of tools and software as well as natively supported by web technologies
2. As semantic vocabularies or ontologies for interoperability and formal specification of the concepts, as necessary for legal interpretation
3. As more concise or practically relevant formats, such as binary representations, based on requirements of the use-case or domains e.g. data constraints within IoT.

Along with identifying the information relevant for assessing and demonstrating the validity of consent, the project also explored the possible means of provisioning this information for the creation and utilisation of receipts within the context of a web browser. For these, the following methods were explored:

1. Specifying information in web-pages directly using JSON or JSON-LD declared using the <script> element.
2. Specifying information in web-pages by specifying the link to an external resource containing the information by using the <meta> element.
3. Embedding information using Microdata or RDFa

This work also explored how notices and consent requests and/or consent decision interfaces (together constituting 'consent dialogues') can be enriched with embedded semantic annotations using both available HTML methods, which uses the <dialog> element for representing notices, and <data-*> elements for indicating information of their locations. The work also explored annotating semantic information by using external vocabularies such as Schema.org or other semantic vocabularies available through the existing research in this area.

This work, in particular the analysis of information requirements from the GDPR and the resulting 'fields of information', are expected to be part of dissemination to external groups by the project members to: ISO/IEC 27560 ongoing standardisation efforts, W3C's DPVCG, Kantara's ANCR working group, and Schema.org.

4 Evaluation

There were two sets of tests regarding evaluation

- functional testing
- and usability/trials tests. at some scale

For the first part, we successfully demonstrated that the PaECG architecture is simple and minimally viable, to be deployed in virtually any website. The feedback obtained, which is included in our paper to [Open Identity Summit 2021](#), is that, with sufficient software integration on the websites and apps, PaECG should be viable beyond the typical difficulties of modifying current software deployments (which is beyond the scope of PaECG itself).

Users also found the software easy to use, based on qualitative informal and non-extensive tests.

Regarding usability and trials tests, the project was unable to proceed at the desired pace. Our plans were to invite a browser maker – Brave - with a known interest in Privacy. The add-on we developed was planned to be natively integrated into the browser and we expected a sizable set of users (in say, 10s) and at least 10 websites to support PaECG receipts.

Due to the unfamiliar operating environment due to the Covid-19 pandemic, we were unable to progress trials.

5 Project Outcomes

1.1. Final Technical Report (this deliverable)

This deliverable represents the work conducted within the PaE:CG project. The dissemination level of this document is public, which enables any interested individual or party to view this document freely and without detriment. It has been made available on the project website¹² and has been deposited to Zenodo for long term availability and archival.¹³

1.2. Open Source Software

The key results of the PaE:CG project are:

- User Agent Plug-in: for assisting people in generating, validating, and managing consent receipts; with code released as open source
- Server component: for assisting data controllers and service providers in generating, validating, and managing consent receipts; with code released as open source
- Consent Gateway: for acting as a trusted third party in the consent receipt process as a witness, and for providing additional services; with code released as open source
- Consent Receipt: a documentation \required for validating and demonstrating the validity of consent in the form of a record of information associated with the consent process; published

The PaE:CG project has made code available for implementing components as a reference and proof-of-concept at: <https://github.com/PAECG/NGI-PaECG-public> as open source under a permissive license to encourage adoption and reuse.

1.3. Contributions to ISO/IEC 27560

The goals of ISO/IEC 27560 Consent record information structure strongly align with those of this PaE:CG project in that they both aim to create a specification for privacy notice records and involve the utilisation of Consent Receipts as their

¹² <https://privacy-as-expected.org/deliverables.html>

¹³ <https://doi.org/10.5281/zenodo.5086239>

basis. Given the topicality of PaE:CG’s work in addressing the requirements of the GDPR in an EU context, and the necessary global abstraction befitting an ISO standard – there is no full overlap in utilising the PaE:CG to directly work within the ISO standard. This difference notwithstanding, several of the concepts have a corresponding overlap. For those that do not, such as the GDPR-specific concept, their inclusion provides motivation for inclusion of additional information within the Consent Receipt.

Contributions to ISO standards drafts are made by submitting comments and contributions through national standards bodies and liaisons. As of the close of the PaE:CG project in July 2021, ISO/IEC 27560 is inviting comments and contributions on its third working draft. The PaE:CG project has contributed comments to the second working draft early in 2021 via the NSAI (IE) national body and Kantara Initiative (Category C Liaison). Selected outputs of this project, including this deliverable, will be submitted through the same channels as well as BSI (UK) to the third working draft whose deadline for accepting contributions is in August 2021.

1.4. Kantara, Advanced Notice and Consent Receipt Working Group

This deliverable will also be an input to the Advanced Notice & Consent Receipt Working Group (ANCR-WG)¹⁴ within Kantara, which has continued the Consent Receipt Specification with the aim to unify the semantic elements to produce a V2 Consent Receipt Information structure.¹⁵ The leadership of ANCR-WG consists of PaE:CG project members who will oversee the transfer of information and its utilisation within the scope of the WG. The ANCR is chartered to “publish a Notice Record and Consent Receipt Specification as a conformance assessment tool to address the technical gaps in the current (v1.1) specification and include recent standards and other technical and legal developments.” with specific objectives in updating the consent receipt v1.1 and incorporating ISO/IEC 29184 requirements. This deliverable provides valuable work for both objectives.

1.5. W3C Data Privacy Vocabulary CG

This deliverable will be an input to W3C’s DPVCG¹⁶ as suggestions to improve DPV in addressing its fields for representing information about consent. More specifically, the ontological notation and legal references are of interest to the group given its overlap with the concepts in DPV. Members of PaE:CG are also active members of the DPVCG and will initiate and oversee the contribution.

¹⁴Kantara Initiative, ANCR WG Home page,

<https://kantarainitiative.org/confluence/pages/viewpage.action?pagelId=140804260>

¹⁵Kantara Initiative, ANCR WG “Consent Receipt v1.2: Anchored Notice Record and Consent Receipt”, <https://kantarainitiative.org/confluence/pages/viewpage.action?pagelId=144016373>

¹⁶ W3C Data Privacy Vocabulary Community Group, <https://www.w3.org/community/dpvcg/>

1.6. Schema.org

Currently, schema.org does not provide any concepts related to consent or even commonly used concepts such as privacy policies, controllers, terms and conditions, notices, and so on. This perhaps reflects its focus on providing concepts only of interest within SEO applications. However, PaE:CG project members consider that even information such as legal identity, privacy practices of a website, and the availability of such information is a matter of interest and importance for search engines and has application beyond merely the generation of consent receipts, to annotating privacy policies to enable search engines (and authorities, researchers, and machines) to extract information and answer questions for the layperson.

For this reason, PaE:CG project members propose this work to form the basis for initiating discussions and suggesting concepts for inclusion in schema.org or the creation of an extension for providing legal concepts for use in web pages. The existing LegiCrowd¹⁷ project has similar goals and provides direction for the application envisaged. LegiCrowd specifically addresses consent¹⁸ in three types - explicit, implicit, and for minors and uses the GDPR as its source for the concepts.

1.7. Workshop on Consent

To further fulfil the dissemination objectives of the PaE:CG project, project members successfully organised an “International Workshop on Consent Management in Online Services, Networks and Things” (COntSeNT)¹⁹ within the IEEE European Security & Privacy Conference.

The workshop is scheduled to be conducted alongside the main conference on September 7th 2021 in a virtual setting. The workshop will consist of presenting academic as well as discussion papers, a keynote by Dr Johnny Ryan FRHistS (ICCL), and a panel discussion consisting of members: Hielke Hijmans (DPA, Belgium), Irene Kamara (Tilburg university), Mark Lizar (Kantara Initiative), Robin Berjon (New York Times), Rob van Eijk (Future of Privacy Forum), Townsend Feehan (IAB Europe).

1.8. Privacy as Expected (for Parental Consent) - Workshop on Global Code of Conduct for Parental Consent

To further fulfil the dissemination objectives of the PaE:CG project, project members are involved in the Children’s Digital Rights Council²⁰ - July 28th 2021 Workshop for leaders in children's privacy, standards, and trust, inviting world renowned experts to team up and solve some of the toughest governance challenges humans may ever face. It is focused on re-defining privacy with the rights of the child being the focus rather than just the Parental. Proposing PaSE

¹⁷ <http://www.legicrowd.org/>

¹⁸ <http://www.legicrowd.org/schema/schemahierarchy.php>

¹⁹ <https://privacy-as-expected.org/consent2021/>

²⁰ <https://accessprivacy.org>



for Global Privacy Rights Access to support a universal approach to improving online privacy rights access.

1.9. Publication of Research Outputs

This project's outputs have been influenced through the following publications funded by the PaE:CG project:

1. "Comparison of notice requirements for consent between ISO/IEC 29184:2020 and GDPR" by Harshvardhan J. Pandit and Georg Philip Krog. Published in *Journal of Data Protection & Privacy* vol.4 issue.3 (2021). <https://www.henrystewartpublications.com/jdpp/v4>
2. "Crowd-sourcing Multi-Domain Issues in Consent Dialogues for Automated Generation of Legal Complaints" by Harshvardhan J. Pandit*, Brian Lynch, and Dave Lewis. Presented at *CHI Workshop on Dark Patterns in Design: What Can CHI Do About Dark Patterns? (DarkPatterns)* - co-located with ACM Conference on Human Factors in Computing Systems (CHI 2021). <https://doi.org/10.5281/zenodo.4553324>
3. "[How] Do Users Benefit From Giving Consent?" by Harshvardhan J. Pandit, Soheil Human, and Mandan Kazzazi. Presented at *Workshop on Technology and Consumer Protection (ConPro)* - co-located with IEEE Symposium on Security and Privacy (IEEE S&P 2021) <https://doi.org/10.5281/zenodo.4601141>
4. "Role of Identity, Identification, and Receipts for Consent" by Harshvardhan J. Pandit, Vitor Jesus, Shankar Ammai, Mark Lizar, Salvatore D'Agostino at *Open Identity Summit 2021 (OpenIdentity)* <https://dl.gi.de/handle/20.500.12116/36495>
5. "Consent Through the Lens of Semantics: State of the Art Survey and Best Practices" by Anelia Kurteva, Tek Raj Chhetri, Harshvardhan J. Pandit, Anna Fensel. Published in *Semantic Web Journal* (forthcoming, 2021). <http://www.semantic-web-journal.net/content/consent-through-lens-semanticsstate-art-survey-and-best-practices>

Additionally, the following publications acknowledge the PaE:CG project and its work as a source for funding:

1. "Building a Data Processing Activities Catalog: Representing Heterogeneous Compliance-related Information for GDPR using DCAT-AP and DPV" by Paul Ryan, Harshvardhan J. Pandit, Rob Brennan at International Conference on Semantic Systems (SEMANTiCS). (to be presented) paper archived at: <https://hdl.handle.net/2262/96594>
2. "ODRL Profile for Expressing Consent through Granular Access Control Policies in Solid" by Beatriz Esteves, Harshvardhan J. Pandit, Victor Rodriguez Doncel at Workshop on Consent Management in Online Services, Networks and Things (COSeNT) - co-located with IEEE European Symposium on Security and Privacy (EuroS&P 2021). (to be presented)

6 Future Work

6.1 Technical Developments

The project team believes that PaECG broke new ground in terms of the development and adoption of the concept of Consent Receipts. The essential use-cases were defined and implemented in a robust and easy to use prototype. The code is open source.

Through the Kantara Initiative's ANCR WG and ISO Board of Trustees Liaison Sub-Committee project team members were able to channel more than a decade of community interest in consent and information sharing into this project.^{21, 22, 23} and through the PaECG project's contributions to Kantara, PaE concepts and components can be contributed back to ISO/IEC 27560 in comments due Aug 16 2021.

In the immediate future, we hope to continue this work through:

- running large scale trials inviting key industry partners, websites/apps and users
- implementing the remaining use-cases -- notably, the use case that keeps third-parties accountable.

It is worth noting that the PaECG project also only tackled the problem of static collection of personal data -- such as registration forms. To limit the scope to the time and resources available, it deliberately kept out of scope dynamic scenarios such as cookie-based functionality and dynamic tracking. These are equally important problems and, perhaps, even more crucial in correcting the power imbalance of current online Privacy.

The Open Consent Group and the Kantara initiative has facilitated the development, adoption and start-up of several community efforts and Consent Receipt collaborations, most notably;

- W3C Data Privacy Vocabulary WG, where critical consent record and receipts semantic challenges have been addressed.
- The My Data Global Community, originating in the OKF open-data mydata work group. The Consent Gateway was born out of participation in the

²¹Mark Lizar, Monvoisin & Givotosky, 2007 Identity Trust Charter @ Identity Commons
http://wiki.idcommons.net/Identity_Trust_Charter

²² Kantara Initiative Consent & Information Sharing WG 2015-2019
<https://kantarainitiative.org/confluence/display/archive/WG+-+Consent+and+Information+Sharing+-+CISWG>

²³ Kantara Initiative ANCR-WG, (2020) Consent Notice Receipt v1.2 Record and Receipt Framework,
<https://kantarainitiative.org/confluence/pages/viewpage.action?pageId=144015859>

MyData community, evolving a Kantara Consent Receipt presentation into a winning series of hackathons²⁴²⁵ for universal MyData controls.

6.2 Future usability with GDPR

The PaE protocol as defined in this deliverable can be adopted as a 'delegated act' as defined in Article 12.8 for the purpose of the Data Subject and PII Controller demonstrating compliance with Article 30, Records of Processing,²⁶ offering Proof and evidence that a Data Subject had a choice by virtue of using a Consent Receipt, thereby also assisting those that co-regulate the processing of personal data.

With the above in mind two near term activities are being considered:

- One of the PaE:CG project partners (Open Consent Group) is looking to further develop the PaE protocol by applying for upcoming EU funding in NGI Atlantic and Horizon Europe
- Working towards a submission to the European Data Protection Board (EDPB), requesting a review of the PaECG protocol to be adopted as a 'measure' for a 'delegated act' of authority, (Article 12.8);
 - To authorize the use of the PaECG protocol for consent driven data portability mechanisms and required privacy risk assurance for Data Subjects in the European Digital Single Market.
 - To operationalize Identity Governance Authorities with a Consent Gateway Controller Register of notice standards and conformant Codes of Practice (a.k.a Certification of Trust Assurance or Trust Registrar) operated by industry trade organizations with verified claims used to establish digital identity assurance between federated identifier ecosystems.

Future Interoperability

Continued work on the Consent Receipt works in the Kantra Initiative ANCR workgroup includes the specification of the consent gateway api protocol for privacy claims that can use by automatically used in digital identity protocols for authorisation and authentication, to be able to set permissions for data processing that are more reasonably what people expect.

²⁴ Joss Langford, 2016 - Consent Gateway - MyData UltraHack Finals, <https://www.youtube.com/watch?v=O8Gzs0Dqc3Q> [Joss is also Chair of COEL TC at OASIS)

²⁵ Mark Lizar, Consent Receipt Gateway 2016 3rd competition Final Round, <https://youtu.be/95pYF2ohAbU>

²⁶ GDPR, Article 30,1 'Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility.' Which the Data subject can do privately while sharing the performance of access to rights



- UMA Work Group²⁷ for User Managed Access protocol that can implement and validate the scope of rights and access to resources
- FAPI (Financial Application Programming Interface, <https://openid.net/wg/fapi/>) with OpenID
- GNAP - Grant Negotiation and Authorization Protocol <https://datatracker.ietf.org/wg/gnap/about/> developing in the IETF, the next generation internet identity management protocol.

With this approach, the PaE protocol can be useful as a conformity assessment tool for use with national iD schemes and frameworks such as:

- eIDAS - European Identity Framework
- UK Digital Identity Schemes
- NIST - US internet and cybersecurity trust assurance
- DIACC - Pan-Canadian Trust Framework

Laws, Standards & Technical Communities

Privacy as Expected is based on an extremely well- established legal test for the application of privacy rights, derogations and data processing obligations. It leverages the fact that the reasonable expectation of privacy is an element of privacy law that determines in which places and in which activities a person has a legal right to privacy, and how people can access these rights with consent.

This legal test is reflected in tort law around the world and in the EU is very well substantiated through case law and the European Court of Human rights act Article 8, Right to Respect for Family and Private life. ²⁸ In which the reasonable expectation of privacy is a well established right.

In this regard, these laws, that require a privacy policy on a website, a sign for surveillance and the like, represent a globally available policy infrastructure for consent to operate PaE using the Consent Gateway.

This includes the multi-national regulation and conventions like the GDPR, and CoE 108+, in which there are provisions to enforce privacy. What's more, we extend these laws and legal semantics with standards and specifications from the industry and community technical committees.

²⁷ Kantara Initiative, 2021 User Managed Access WG, (UMA_WG)
<https://kantarainitiative.org/confluence/display/uma/Home>

²⁸ https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf



Annex - Technical Communities

ISO/IEC 29100 Privacy and Security Techniques

ISO/IEC 29100 is an international semantic foundation for extending data sovereignty online. It is an open ISO/IEC standard (no charge). This made possible the development of the consent receipt into a purpose specification protocol. It meets the need for a standard semantic framework for the Internet for defining roles of privacy stakeholders for data portability, control and liability in between regions and jurisdictions

An international (and intra- national) technical privacy and security framework used for international governance interoperability providing data control alternatives to standard contractual clauses. .

Semantic Terms Mapped

- In the ISO/IEC 29100 the Data Controller and PII Controller are specified as equivalent terms and privacy stakeholder roles. In addition, the Data Subject and the PII Principal are also equivalent.. (ref)

ISO/IEC 29184 Online Privacy Notice and Consent

This standard consists of a sub-framework of notice content controls to address semantic dark patterns in consent notice, notification and disclosure structure. Annex B publishes the Consent Notice Receipt v1.1 (circa 2015) which was developed in interactions that synced with the the 5 year development of 29184, in which the Kantara Initiative ISO Liaison had an active role commenting on its development.

Semantic Terms Mapped

The ISO/IEC 29184 standardizes a generic version of the legal justifications in the GDPR. These justifications are critical infrastructure for computational privacy and data governance interoperability.

Six categories of legal justifications to layer

- Consent
- Contract
- The vital interest of the PII Principal
- The interest of Public Safety and Security
- The legitimate interest of the PII Controller
- A Legal Obligation

PaECG protocol application:



The flow of use for PaE protocol is human centric and requires strict adherence to human centric semantics. This is not the current service (or user) centric semantics, and is distinctly recognized in this manner.

- The PaECG protocol asserts consent (and democratic consensus) as the primary paradigm in which the other legal justifications transparently operate with reciprocal (risk driven) accountability and proportionality.
- Multiple legal justifications for processing can and do happen at once
 - a. For access to privacy as a service, the use of a right associated with consent, when asserted online can effect many processors, joint controllers, and 3rd parties in different legal jurisdictions,
 - b. A grant of consent for a purpose, is defined here as a specific technical scope for digital identity protocols to use to implement access with identifier management and security.
- Legal Derogations
 - a. Derogations are applied to the consent paradigm as an overlay, and in the PaECG protocol with an overlay capture architecture.
 - b. This enables dynamic data controls for emergency situations, break the glass scenarios, data breach, parental consent, the protection of children by the state, fraud, criminal surveillance and the like, with the protections of Individual baked in.
 - For a meaningful consent receipt, a notice of risk includes whether derogations exist or not.

ISO/IEC 27560.3 Consent record information structure

- Adopted from the Kantara Initiative - Consent Receipt v1.1 in 2019 and voted to standard (29184) in 2020.
- The Open Consent Group has led the efforts at the Kantara Initiative to author and develop the consent receipt.
 - a. CISWG v 1.1 Consent Receipt
 - b. ANCR v 1.2.1 - Notice Record and Receipt framework for the 29184 Consent Notice Receipt (in draft)²⁹

W3C Data Privacy Vocabulary Controls Community Group (W3C DPV CG)

Data Privacy Vocabulary Controls is a Community Group³⁰ chaired by Harshvardhan Pandit (our team member). Presenting a legal ontology that is technically specified for semantic use both human understandable and machine readable. Developed with active participation of the German Data Protection Office and technically used with semantic protocols like RDL, OWL, RDF etc.

²⁹ Where the Privacy as Expected CG protocol has been contributed for input as a comment to the 27560 committee.

³⁰ W3C, Data Privacy Vocabulary Community Group
<https://www.w3.org/community/dpvcg/>



The DPV adopted the consent receipt format and ISO vocabulary in v0.2³¹ of the DPV published in 2019.

- Originating from the SPECIAL³² the DPV CG was launched at the Open Data Institute on the eve of the GDPR. Hosted by the Kantara Initiative CISWG WG³³ and MIT Media Labs ([live recording](#)) in Boston.
- A significant point is that the DPV can now be used for human and machine readable records, and with PaE signalling, proof of human understandable consent which can enable high risk privacy transparency and compliance.
- The DPV as it is provided, does not recommend any specific way to use its concepts. Adopters are free to utilise their preferred models (e.g. RDFS-style, OWL2-style, or simply as a list of terms),
- The PaECC utilises the DPV to specify purpose, notice, notifications and disclosures in the PaE protocol. It is the interaction with Notice that generates a Consent Receipts. Memorializing service notification and interaction to personalize privacy for people.
- Utilizing standard semantics to automate privacy rights informance access and access performance monitoring.

OASIS COEL - Classification for Everyday Living

- An industrial standard from OASIS³⁴ in which a data governance authority is used to capture contextual attributes into event based atoms.
- A WG effort at OASIS with roots in the monumental work that OASIS contributed to the development of international guidelines and standards. OASIS IPR as well as semantics are derived from the consent receipt v0.7 are interoperable..
- COEL interoperability is seen in the ability to extend the Consent Gateway with an atom based public data store which only the PII Principal can aggregate, but all stakeholders can use for analytics and deep/big data insights,

Trust over IP: Notice & Consent Task Force

- The V1 Draft of the Controller Notice Credential³⁵ is under way in the Inputs and Semantics WG. The assertion of the controller and contact information is a required PaECC security component. It specifies the use of the PaECC

³¹ W3C DPV, (2021) Data Privacy Vocabulary v0.2, <https://dpcvg.github.io/dpv/>

³² SPECIAL Project, <https://www.w3.org/2018/vocabws/report.html>

³³ Kantara Initiative + W3C DPV + MIT Media Labs (May 24, 2018) End of Privacy 1.0, Workshop, K W3C DPVCG Launch event https://kantarainitiative.org/confluence/download/attachments/3408008/May-24_-End-of-Privacy-1.0-Report-2018.pdf?version=2&modificationDate=1528791074000&api=v2

³⁴ COEL, Classification of Everyday Living https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=coel

³⁵ Controller Notice Credential; <https://wiki.trustoverip.org/pages/viewpage.action?pageId=72225>



protocol stack by a 'user agent' to generate a digital twin of the privacy notice, in the form of ANCR Record³⁶, which is then used to generate a consent receipt.

- When using the PaECG protocol the Consent Gateway cannot be accessed without a verified Controller (Notice) Credential . This initial point of discovery is required for self asserted access to privacy rights information.
- The Privacy Controller Credential (PCC) comprises the legal to technical requirements for Privacy Assurance, and is intended to be extended by the self-sovereign (consent authorized) use of verified claims as digital identity identifiers.

Blinding Identity Taxonomy: Kantara Initiative³⁷

- A Kantara publication, the taxonomy is used for securing PII by one way linking Consent Notice Receipts so that only the Data Subject can be the Master ANCR Record Controller and Aggregator of its receipts.
- Useful for the safe storage of Consent Receipts. Dramatically lowering the privacy impact of identifier surveillance and security of digital privacy risks. While increasing the capacity to produce verifiable claims for single market capable services like self-advertising.
- De-risking the access, use and processing of personal data for dynamic data controls with multiple stakeholders and legal justifications. A contribution from the Human Colossus foundation.³⁸

³⁶ The first record of the digital identifier relationship captured with the protocol is an anchored, notice and consent receipt record, and is used to generate and validate the state of consent.

³⁷ Blinding Identity Taxonomy

<https://kantarainitiative.org/download/blinding-identity-taxonomy-pdf/>

³⁸ The human colossus foundation is an NGO, a non-profit focused on developing global schema semantic architecture with capture overlays, led by Paul Knowles, who is also the chair of ToIP: Inputs and Semantics WG, engineering global semantic interoperability infrastructure, developing a dynamic data system overlay capture architecture