Engaging Content
Engaging People

CC BY NC

Role of Identity, Identification, and Receipts for Consent

Privacy as Expected: Consent Gateway (PAECG) Project funded by NGI TRUST

Harshvardhan J.Pandit | pandith@tcd.ie | @coolharsh55
ADAPT Centre, Trinity College Dublin, Ireland

Vitor Jesus, Shankar Ammai
PrivDash Ltd., United Kingdom | (former: Birmingham City University, UK)

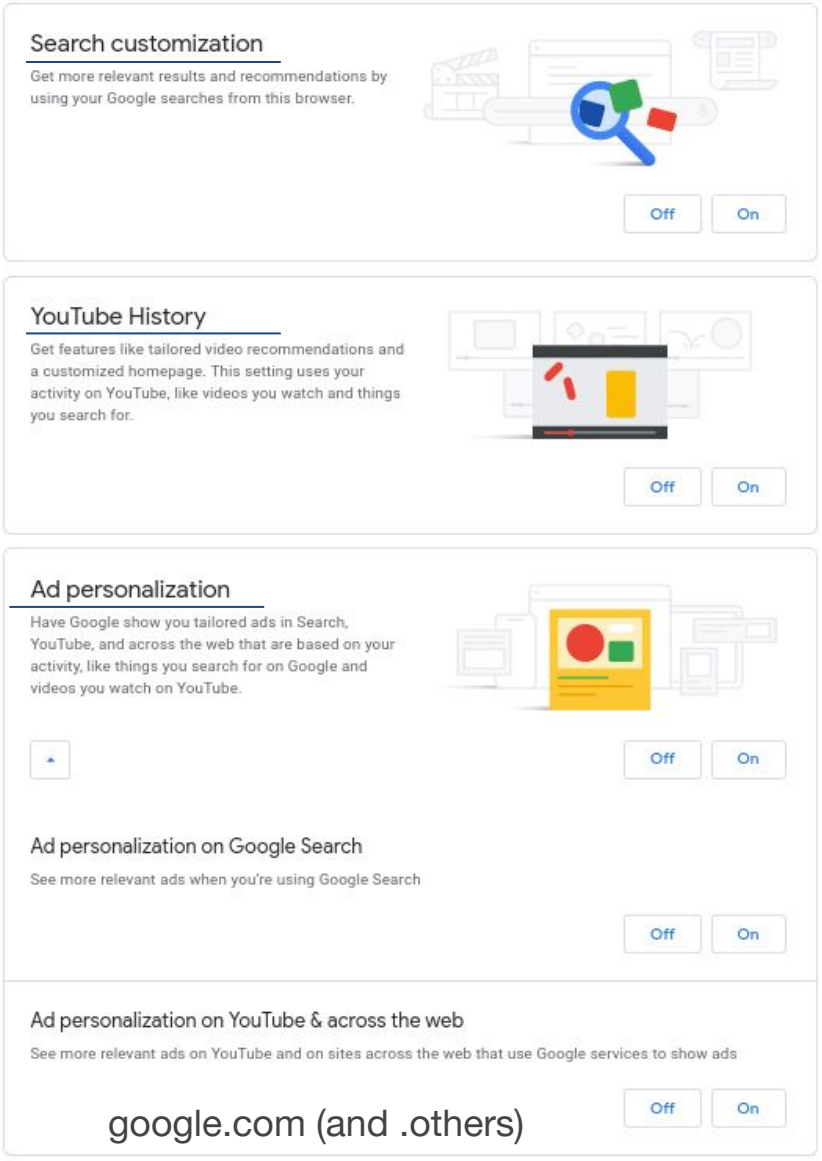
Mark Lizar, Salvatore D'Agostino
OpenConsent, London, United Kingdom

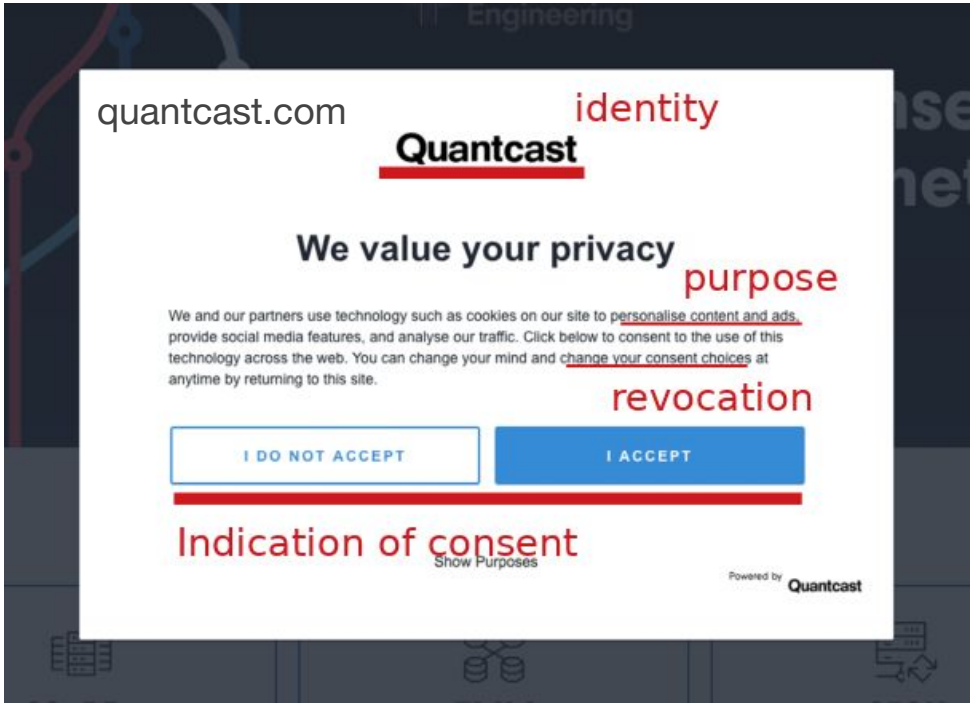
This work has been funded under the European Union's Horizon 2020 research and innovation programme NGI TRUST Grant#825618 for Project#3.40 Privacy-as-Expected: Consent Gateway. Harshvardhan J. Pandit is also funded by Irish Research Council Government of Ireland Postdoctoral Fellowship Grant#GOIPD/2020/790; and ADAPT SFI Centre for Digital Media Technology funded by Science Foundation Ireland through SFI Research Centres Programme and co-funded under European Regional Development Fund (ERDF) through Grant#13/RC/2106_P2.

Trinity College Dublin, Coláiste na Tríonóide, Baile Átha Cliath, The University of Dublin
BIRMINGHAM CITY University
OPEN CONSENT
IRISH RESEARCH COUNCIL An Chomhairle um Thaighde in Éirinn
Ireland's European Structural and Investment Funds Programmes 2014-2020 Co-funded by the Irish Government and the European Union
European Union, European Regional Development Fund
SFI

The ADAPT Centre is funded under the SFI Research Centres Programme (Grant 13/RC/2106) and is co-funded under the European Regional Development Fund.

Consent on the Web: An Interactive Contract





Consent should be:

- Freely given → without coercion, no obligation
- Specific → exact and limited in scope
- Informed → prior knowledge
- Un-ambigious → clear indication of consenting
- Revocable → once given, can be withdrawn

- GDPR Art. 4-11 (2016)

Identity and Consent

GDPR says:

1) Collect valid consent (legal requirements)
2) **Provide ability to withdraw given consent**
3) Provide rights (applicable to certain contexts)
4) **Don't collect additional information**
   e.g. to validate identity merely for the purposes of identification for consent (data minimisation)

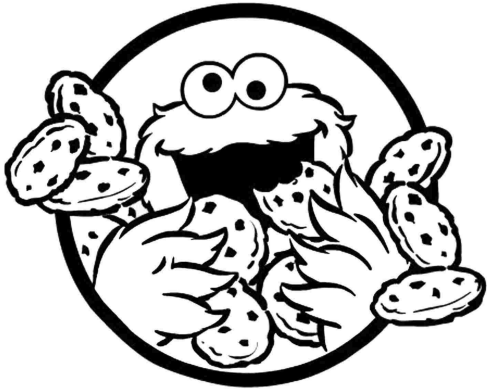
Resulting scenario:

- If user has an account, consent is tied to the account
- If user does not have an account, how to handle consent?
- If temporary identifiers are utilised, how to do data minimisation?

Two biggest challenges

Cookies (default choice for local data management for the web)

- Ephemeral storage → collect universal consent with local control
- Non-transparent → opening the cookie jar requires expertise
- Non-transferable → cookies are per device, per app, per profile
- Conditional → if no cookie, no control of preference
- Lack of control → no user-utilisation of cookie or cookie-data
- Non-challengeable → no user-ability to verify or challenge
- Un-manageable → browsers only give ability to delete cookies



Notices:

a) (privacy is the) “biggest lie on the internet” -- [OO20]

b) the web is full of dark patterns and malpractices -- [SBM20, Ur20]

Technical approaches deployed (optional slide)

Do Not Track (DNT) → boolean (set on / off) browser signal to indicate user does not want to be 'tracked' across the websites. Last standardisation via W3C in 2019. All browsers implement it. No websites it. Spectacular failure. https://www.w3.org/TR/tracking-dnt/

Global Privacy Control (GPC) → boolean (set on / off) browser signal to indicate user does not want their data to be 'shared' beyond the website/controller. Last specification Jan 2021. Only 1 browser currently implements it - Brave. Some websites support it. Legally enforceable under CCPA. Uncertain regarding GDPR[1]. https://globalprivacycontrol.github.io/gpc-spec/

Privacy Labels → Apple introduced notices for its App Store which requires developers to post information about data collected and used for tracking of individuals, in addition to requiring them to ask consent for tracking - and provides a global setting to prohibit such requests. The company dogfoods: https://www.apple.com/privacy/labels/

1 GPC + GDPR: will it work?. Harshvardhan J. Pandit. 2021. https://harshp.com/research/blog/gpc-gdpr-can-it-work

Consent Receipt

1) A ***consent receipt*** is similar in principle to a record of transaction issued as a receipt, whether in grocery stores, or shopping websites.

2) Kantara published Consent Receipt (2018) specification outlining a schema for issuing 'receipts' for given consent.
   a) How to deploy? Does it meet legal requirements?
   b) ANCR working group (2021) initiated to upgrade spec.

3) ISO/IEC 29184 (2020) standard for online privacy notices for consent
   a) mentions possibility of machine-readable metadata.
   b) ISO/IEC announced 27560 (likely publication >2023) as an upcoming standardisation effort for consent receipts.

4) "Web of Receipts": using receipts as proof and record of transactions, and establishing trust through transparency and accountability [Je20]

CC BY NC

Identity, Identification, and Receipts

Two problems with the way consent works today:

1) Consent records do not concern authentication or verification of entities and information → they are only data records
2) Creating receipts requires proactive participation by Controllers

Three challenges that need to be addressed to solve this:

a) Any entity must be able to create its own records
b) Receipts must be capable of specifying and verifying identity
c) Avoiding ‘my word against yours’ type of situations

CC BY NC

The PAECG solution

PaE:CG is a project funded under NGI TRUST (OCT-2020 to JUN-2021) that provides an end-to-end, user-centric, comprehensive, open source solution to managing Consent for Personal Data.

The driving principle for PaE:CG is utilising receipts for an accountable mechanism while ensuring the Internet as it currently is and should remain for the most part a pseudo-anonymous space, while still empowering individuals with choice and control through consent.

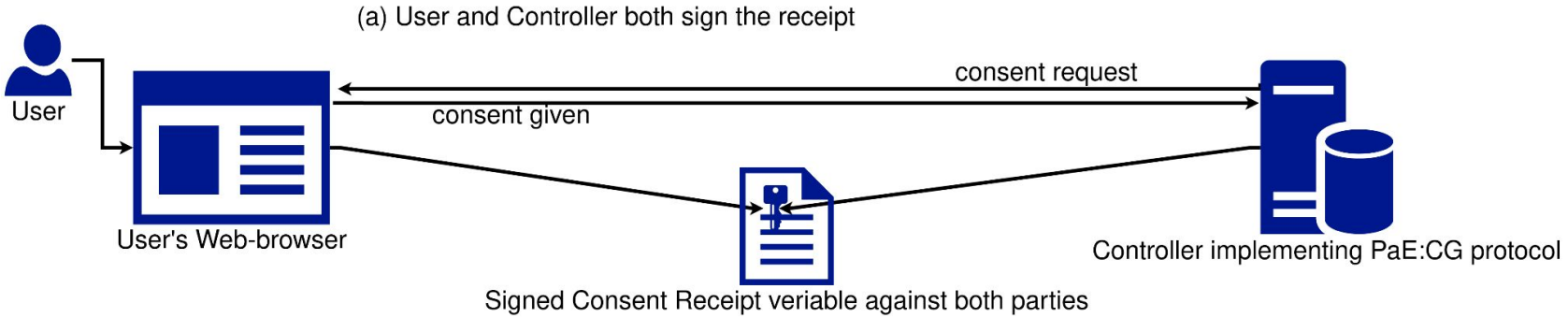
- Consent interaction → Consent Receipt
- All parties must benefit from receipts regardless of participation
- Receipts are cryptographically signed for assurance & verification
- Novel concept of ‘Consent Gateway’ as a Notary or Witness

Receipt → Identity → Identification

- PAECG protocol :: implementation of developed solution
- Receipt uses bearer tokens to provide cryptographic guarantees regarding identity when receipts are generated and signed
- Receipts *can be* a form of De-centralized Identifier (DID)
- Therefore, receipts can be utilised to provide an *identifer* for identification in interactions, e.g. consent withdrawal
- Receipts, by acting as an identification mechanism, can also be used wherever identity is required, e.g. rights exercising

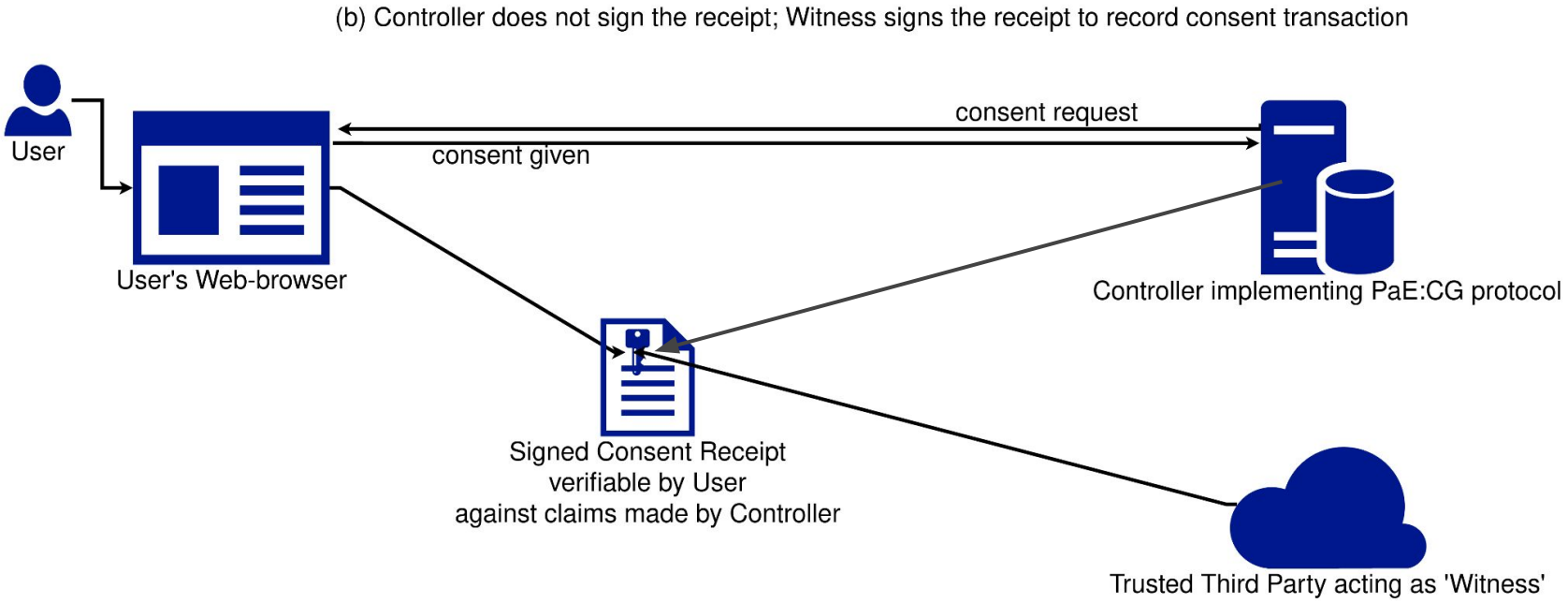
- Controller benefits by having verifiable records, non-invasive identifiers for consent and rights management
- Users benefits by having proof of consent, and accountable record of their consent interaction

Scenario #1: All Parties utilise PAECG protocols



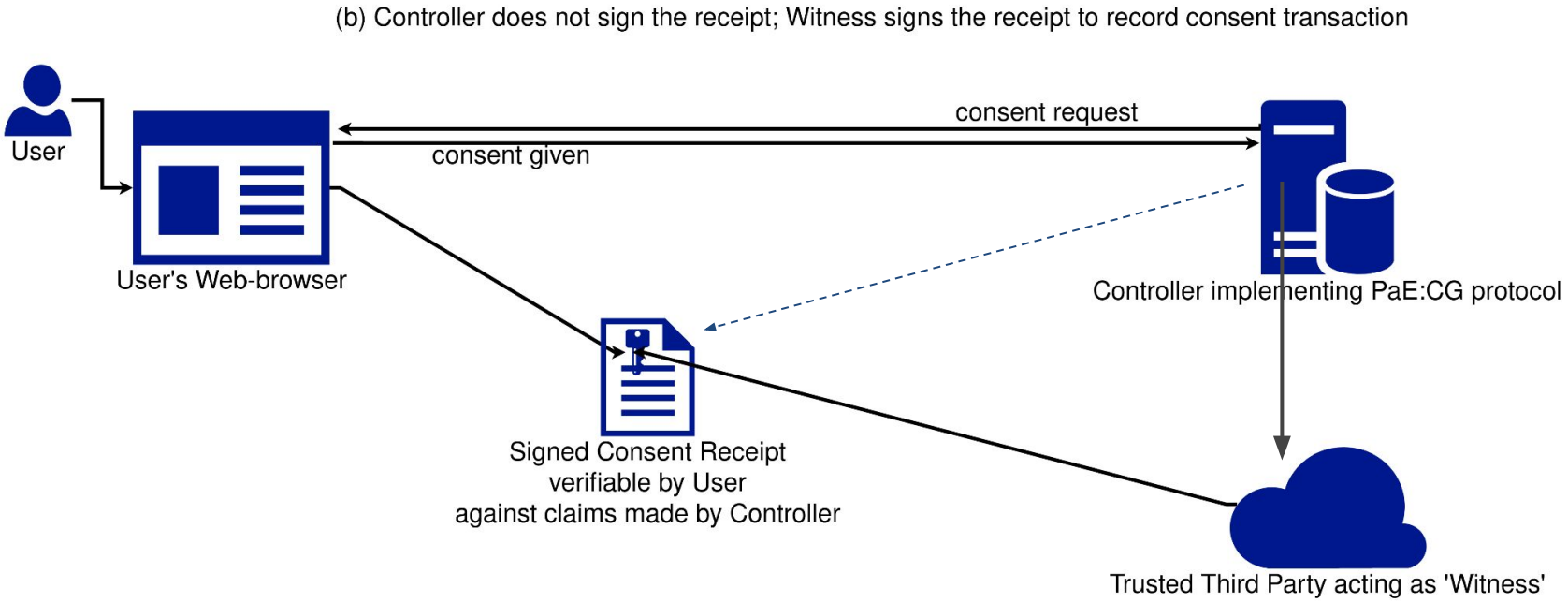
1. User has a browser plugin as *User Agent*
2. Controller implements PAECG protocol on server
3. Both generate Consent Receipt
4. Both sign Consent Receipt
5. Both hold copies of signed Consent Receipt

Scenario #2: CG as Trusted Witness



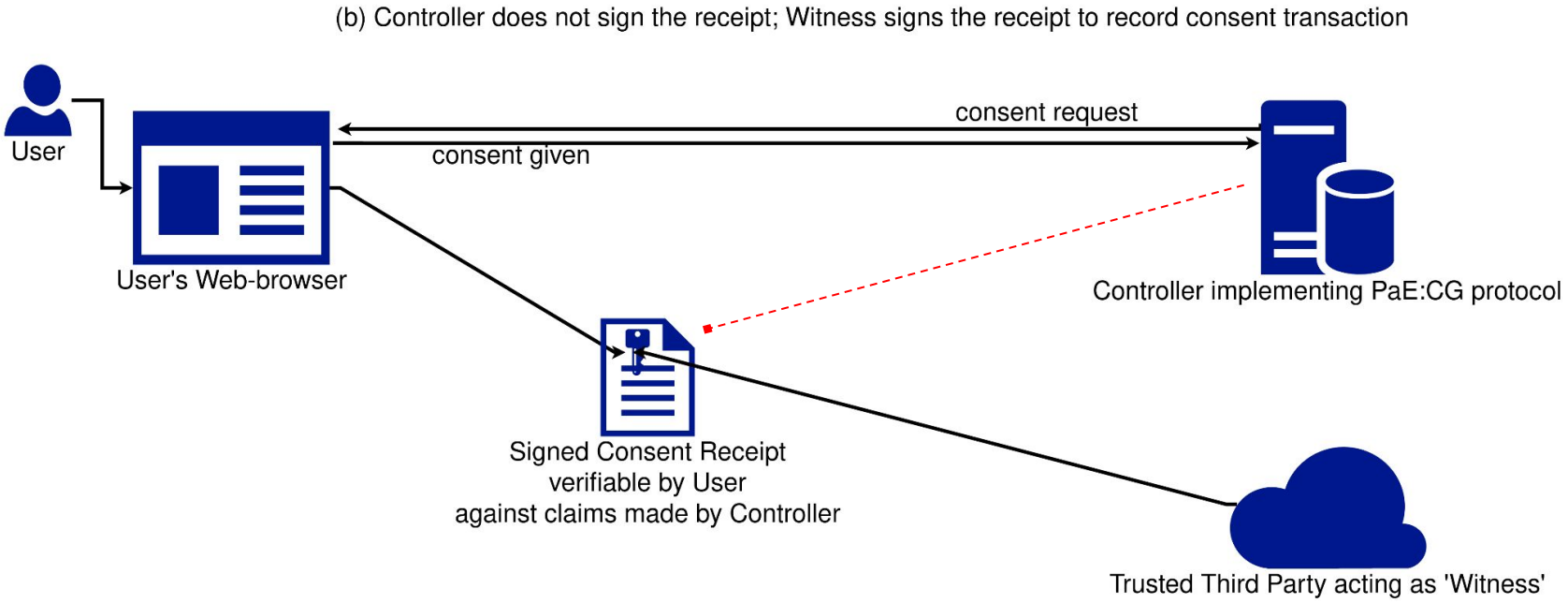
1. User has a browser plugin as *User Agent*
2. Controller implements PAECG protocol on server
3. Both generate Consent Receipt
4. Both + CG sign Consent Receipt
5. Both hold copies of signed Consent Receipt

Scenario #2: CG as Trusted Witness



1. User has a browser plugin as *User Agent*
2. Controller does not implement PAECG protocol on server
3. Both generate Consent Receipt
4. User + CG (on behalf of Controller) sign Consent Receipt
5. Both hold copies of signed Consent Receipt

Scenario #3: Controller does not sign



1. User has a browser plugin as *User Agent*
2. Controller implements PAECG protocol on server
3. User generates Consent Receipt
4. User + CG (as Witness) sign Consent Receipt
5. User has signed Consent Receipt

Information required for Record+Receipt

Credentials / Signing

1) Explicit keys provided by each party
2) Utilise certificates used for websites (e.g. HTTPS/TLS)

Information within Receipt

1) Self-declaration, e.g. website explicitly lists it in web-page
2) Annotated semantics, e.g. website implicitly lists elements which can be extracted from web-page
3) Derived, e.g. take information from consent notices using NLP
4) Provided, e.g. third party public registry of information

CC BY NC

In Conclusion...

- The issue of ‘accountable consent’ is a web-scale problem
- PAECG provides a solution for practical accountability and implementation using cryptographic protocols
- Introduces the novel concept of a ‘Consent Gateway’
- Receipts can be utilised as records of consent, for accountability, legal enforcement, further interactions, identification and authentication, and clarification in disputes.
- Contributions to ongoing standardisation efforts in ISO/IEC, Schema.org, Kantara ANCR, W3C DPVCG, and more.