DIGITAL ADVERTISING TRANSPARENCY & CONSENT MECHANISM

Presented by
Ghita Harris-Newton, Chief Privacy Officer, Quantcast
Matthias Matthiesen, Sr. Manager, Privacy & Public Policy, IAB Europe

FPF Location & Ad Practices Working Group
7 December 2017

iab europe interactive advertising bureau

Technical standard in development and may be subject to changes.

Presentation updated 7 Dec, 2017

Digital Advertising Transparency & Consent Mechanism

- ***IF*** an entity (publisher, advertiser, ad tech vendor) would like to rely on consent as a legal basis to set a cookie and/or process information, this mechanism provides an **industry standard** protocol for communicating and recording that consent.
- This **decentralized** standard leaves **control with the publisher** and
- gives **consumers true transparency and choice**
- while minimizing disruption to ad tech ecosystem.

Background

- Beginning in May 2018, the GDPR will require significant changes for data processing that is based on consent.
- IAB Europe's GDPR Implementation Group ("GIG") has been working on interpreting GDPR consent rules since January 2017 and published its analysis on www.iabeurope.eu.
- The group realized that some of the legal challenges require technical responses, so it has also been developing a technical standard and mechanism to meet GDPR consent obligations.

Why does consent matter?

- Under GDPR, consent is only one of six “legal grounds” for processing personal data, and therefore *not* always needed.
- GDPR also changes the definition of consent applicable to the current ePrivacy Directive, better known as the “Cookie Directive”.
- As a result, much of the cookie-based data collection that the advertising industry engages in will require GDPR consent moving forward.

ePrivacy Directive

NB: The ePrivacy Directive is a law from 2009, not to be confused with its proposed update, the ePrivacy Regulation.

- Storing information, such as cookies, or accessing information stored on a user device requires consent.
- Unless “strictly” technically necessary for provision of the service requested by a user, e.g. shopping cart cookies.

GDPR changes ePrivacy consent

Article 2 ePD
Definitions

f. ‘consent’ by a user or subscriber corresponds to the data subject’s consent in ~~Directive 95/46/EC~~ Regulation (EU) 2016/679.

Article 94 GDPR
Repeal of Directive 95/46/EC

1. Directive 95/46/EC is repealed with effect from 25 May 2018.
2. References to the repealed Directive shall be construed as references to this Regulation […]

ePrivacy rules before GDPR

ePrivacy Consent Requirement

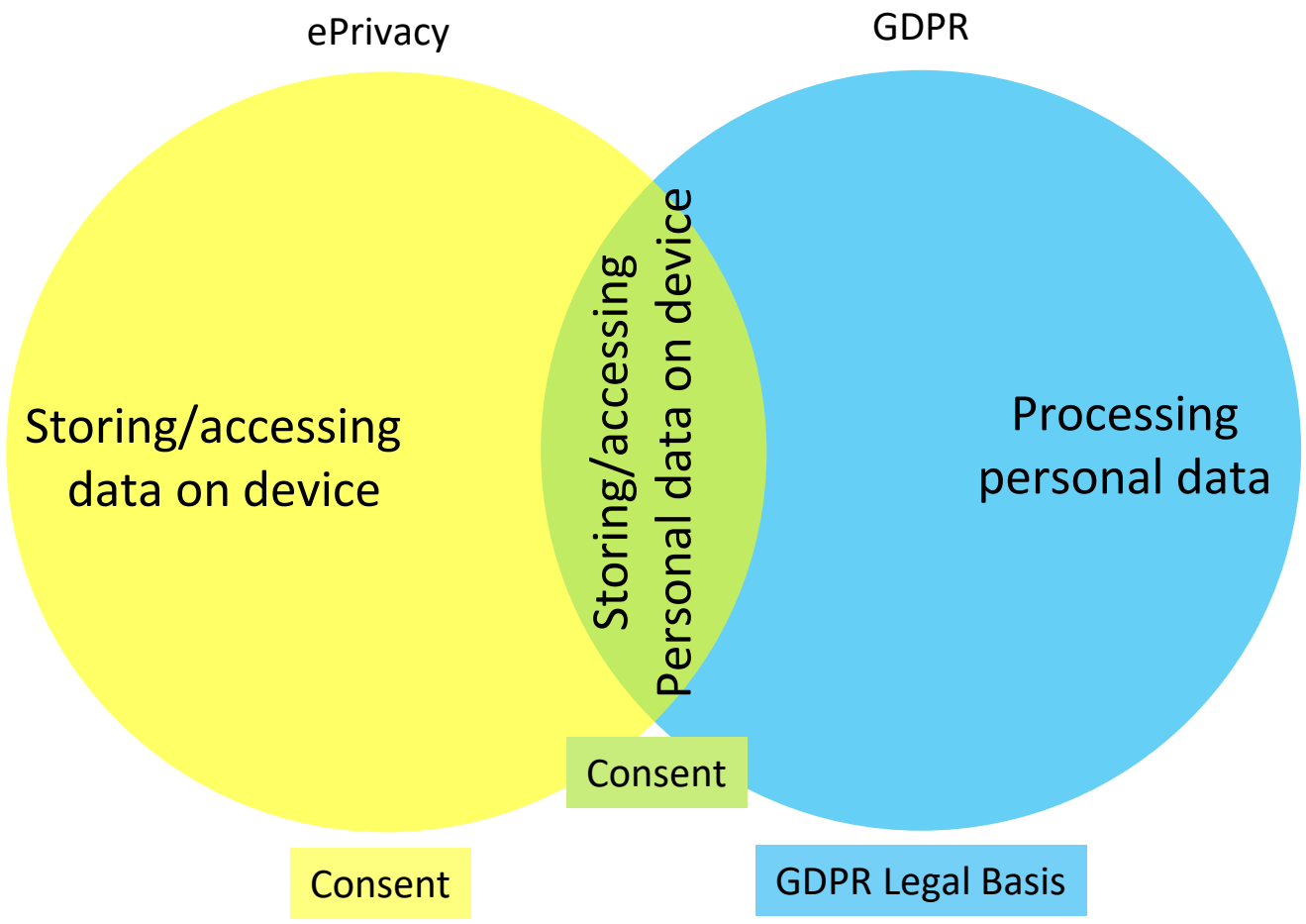
GET CONSENT AS DEFINED BY

ePrivacy rules after GDPR

ePrivacy
Consent
Requirement

GET CONSENT AS DEFINED BY

Hierarchy ePrivacy and GDPR



- Collection of data over the internet generally requires **Consent** because of ePrivacy
- Processing of personal data requires a **GDPR Legal Basis** e.g. consent, or legitimate interest.
- Where both apply at the same time the more specific **Consent** rule of the ePrivacy prevails.

What is GDPR consent?

- Freely given, specific, informed and unambiguous indication of agreement, by a statement or by a clear affirmative action.
- Robust information disclosure requirements, including but not limited to identity of controllers and the purposes of processing.
- Obligation for controllers to be able to “demonstrate” consent, e.g. through a record.
- Revocable as easily as it was to give consent in the first place.

Old consent mechanism inadequate

- Implied consent (by inaction) does not meet the GDPR standard.
- Existing model, where downstream parties assume that consent was obtained on their behalf, may not provide a means to demonstrate consent as required by GDPR for many parties.

What is needed?

- Processing data with GDPR consent will require stronger **cooperation** between and **accountability** by all advertising ecosystem players.
- First parties must **disclose more information** about their own and their third party advertising partners' processing activities.
- Third parties must ensure that first parties have **up-to-date information** for such disclosures.
- If relying on consent, first and third parties must not collect or process information on the basis of consent **before** a user's affirmative consent is given.
- When obtaining consent for itself and its partners, first parties must ensure that it is obtained affirmatively and **communicate** consent choices to third parties.

How do we get there?

Common standards!

- Industry needs common standards; fragmentation will lead to inefficiencies and poor consumer experiences.
- Effective and efficient, neutral industry governance.
- Simple policies around use of the new technical standards to ensure mutual trust and reassurance.

3 Key Points for the Mechanism:

- An **industry-wide** standard in which the ad ecosystem works together to solve the consent requirements of GDPR.
- An **open source solution** that is not driven by any particular company.
- A **publisher centric** tool – **giving consumers the best experience** possible while ensuring that **publishers maintain control** of their sites and generate revenue.

What's the Solution?

"Distributed Registry Chain"

The proposed solution consists of a standard, maintained by a neutral industry entity, that enables the capturing, storing and communicating of consumer consent between publishers, vendors and ad systems.

- Open source, industry-supported
- Distributed technology giving publishers choice
- Limited impact on existing ad ecosystem

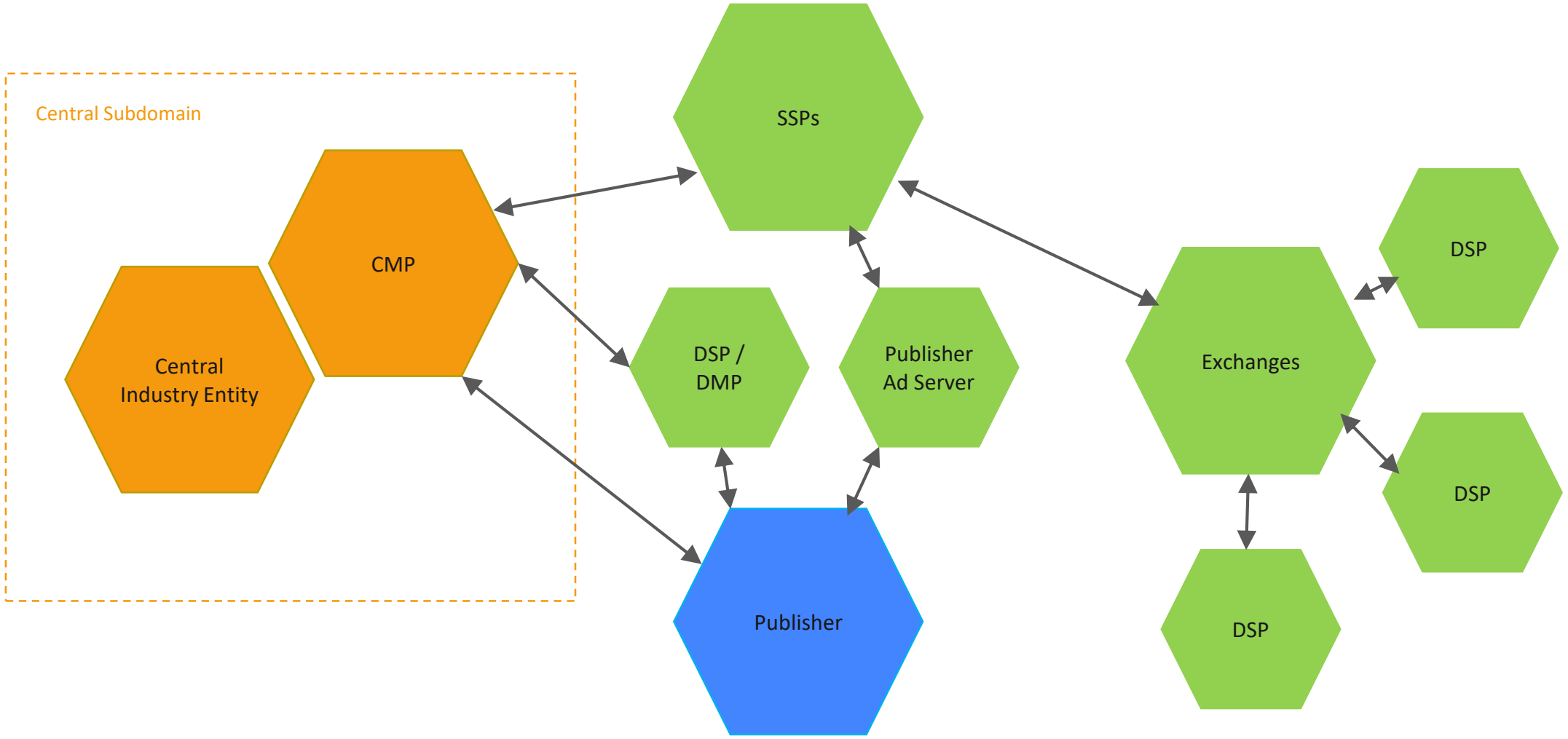
How do we do it?

- New technology standards facilitating and enabling
  - publishers to obtain consent for themselves and on behalf of their partners via standard-based consent management provider;
  - dynamic disclosures with transparency around partners and purposes;
  - communication of consent status between publisher and ecosystem;
  - transparency and choice for consumers, to easily see and modify consent status (including revocation);
  - audit trail proving consent status.
- For desktop and mobile.
- Before 25 May 2018.

Solution Overview

1. **Central Sub-Domain**: leveraged by Consent Manager Providers (CMPs) to manage consent, access a master participating vendor list and support user data access rights.
2. **CMPs:** central entity delegates sub-domains to approved CMPs so that those CMPs can read/write cookies and provide standard APIs that 3rd-parties can query to determine consent status for a given user.
3. **Consumer UX:** CMPs would implement consent UX and consent capture system, leveraging standard APIs as part of their own consent solution on their delegated subdomains for publishers.
4. **Consent Storage:** stored in-browser via 3rd-party cookie (for now); CMP APIs can be queried directly by SSPs to pass consent status down chain for ad serving. This will be improved over time and can easily be swapped out.
5. **Publisher Consent:** supported by CMP UX and API for publishers as needed.
6. **Publisher Control**: publisher maintains control of its site, including whether to seek global (web-wide) consent or service specific (site-wide) consent.

Technical Context



Industry Vendor List

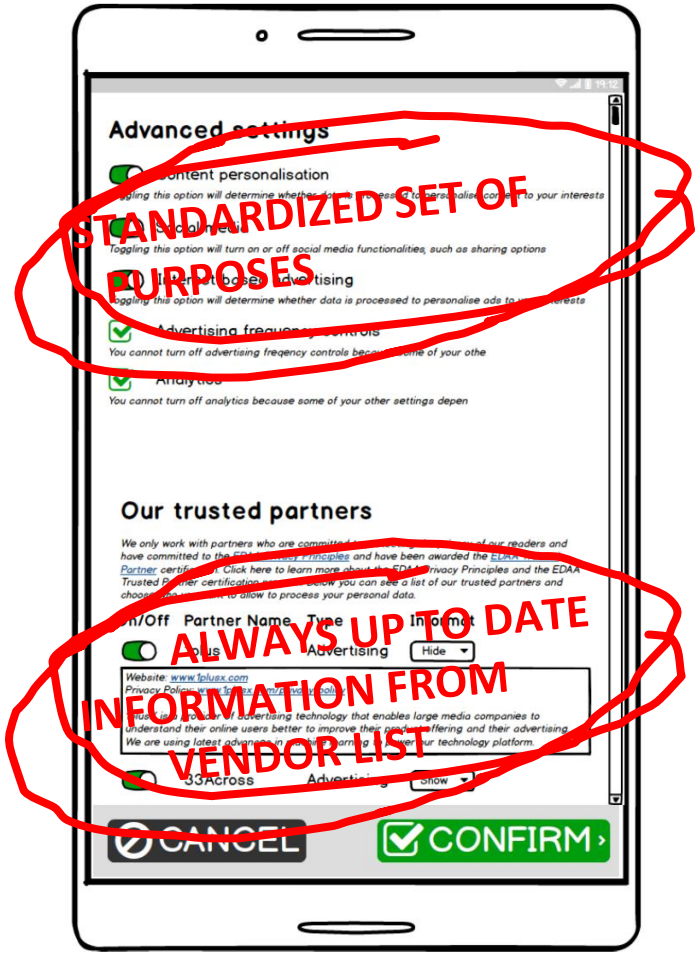
- A centralized, dynamic list of vendors, their purposes, their privacy policy URL, et al
- Versioned to allow for audit trail
- Publishers/CMPs will use the vendor list as basis for disclosure and consent requests
- Both vendors and publishers will need to adhere to baseline principles and minimum standards

ID	Company	Privacy Policy	Purposes	…
1	SSP1	ssp1.de/privacy	1, 2, 3	…
2	ANW2	anw2.be/privacy	2, 3	…
3	ANA5	ana5.fi/privacy	4	…
…	…	…	…	…

ID	Purpose	Description	…	…
1	Purpose 1	domain.eu/purpose/1	…	…
2	Purpose 2	domain.eu/purpose/2	…	…
3	Purpose 3	domain.eu/purpose/3	…	…
4	Purpose 4	domain.eu/purpose/4	…	…
…	…	…	…	…

Requesting Consent

- A JavaScript library/API which enables publishers to customize the experience of asking for consent
  - Abstracts the complexities of consent checking and storage
  - Implements standardized minimum disclosure language
  - Ensures that the vendor list and disclosure language stays updated to latest version
  - Makes the consent data available for downstream usage via daisy chain
- Open Source examples of user interfaces which implement/leverage the API



Storing Consent

- Multiple storage options possible: cookie, mobile app SDK, login alliances, centralized registries, etc.
- Identification required for global consent to be made possible via multiple mechanisms, to be determined via vendors implementing. API will standardize interaction, not implementation.
- First phase to combine cookie-based identification and cookie-based storage / mobile app SDK and AAID/IDFA/vendor ID.
- Over time, the industry could migrate to more resilient storage methods.

Transmitting Consent

- Consent value to be binary: ”consent (1)” or “no consent (0)”.
- Consent will be transmitted via a Daisy Chain: every upstream member will append a consent payload to all downstream requests.
- Consent data structure supports per-purpose (small payload), per-company (moderate payload) or per-company + per-purpose (large payload).
  - Policy requirements and payload size will determine implementation.
- Consent values to be compressed into as small of a data structure possible.

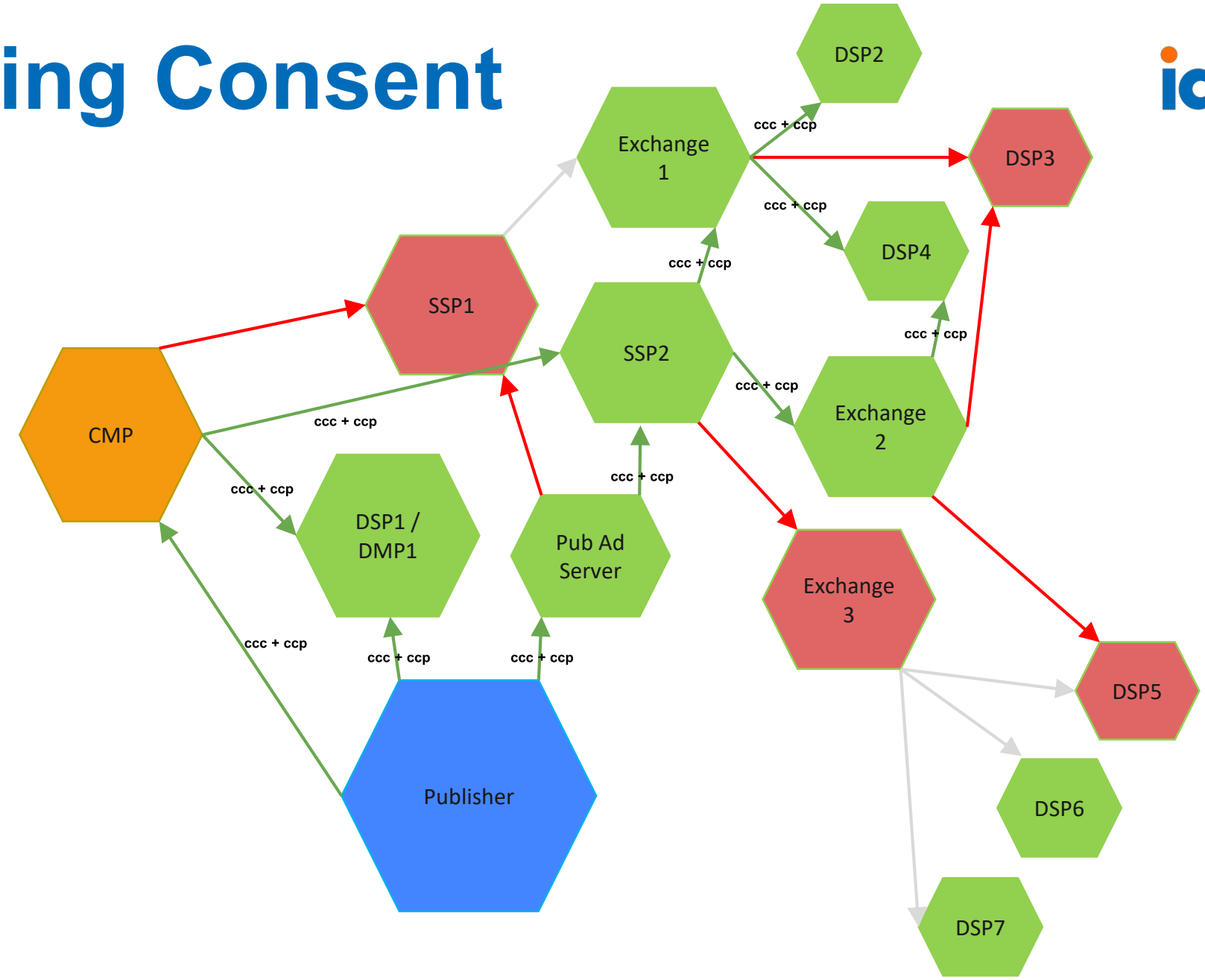
Transmitting Consent

Consent Choices: Controllers (CCC)

- ✓ DSP/DMP1
- ✓ PubAdServer
- X SSP1
- ✓ SSP2
- ✓ Exchange 1
- ✓ Exchange 2
- X Exchange 3
- ✓ DSP2
- X DSP3
- ✓ DSP4
- X DSP5
- ✓ DSP6
- ✓ DSP7

Consent Choices: Purposes (CCP)

- ✓ Pur1
- ✓ Pur2
- ✓ Pur3
- X Pur4



Combined, they enable...

- Transparency into the supply chain for consumers & publishers.
- An auditable consent trail that gives all supply chain members confidence by providing a more efficient disclosure mechanism, enabling companies to ”know” rather than “assume” their consent status with a user.
- A better user experience than if every publisher were to try to solve the challenge on their own.
- Keeping the supply chain that publishers rely on for ad-revenue in tact.

Implementation Targets

NB: Dates subject to confirmation.

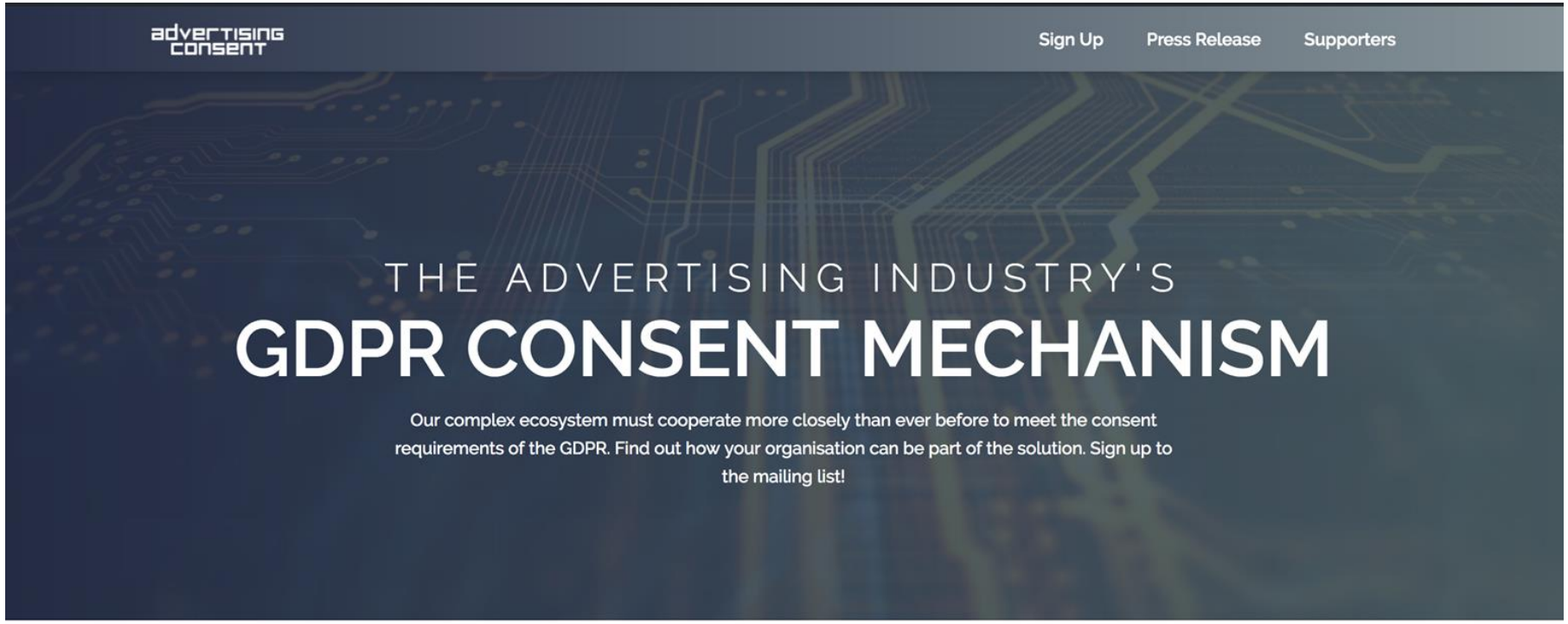
- Publication of technical specifications – December 2017
- Publication of policy standards – February 2018
- OpenRTB Extension specification – February 2018
- Reference implementation – February 2018

Endorsers

Updated 7 Dec 2017 10:30 CET

In anticipation of coming consent requirements in the European market, companies from across the digital media, advertising and analytics ecosystems have been collaborating on a technical approach for storing consumer consent status and sharing this status where appropriate with partners. Our collaboration has produced a framework that the undersigned companies intend to integrate and support in the marketplace in 2018.

Stay informed



www.advertisingconsent.eu

Questions & Answers

Ghita Harris-Newton
Chief Privacy Officer, Quantcast
(gharrisnewton@quantcast.com)

Matthias Matthiesen
Sr. Manager, Privacy & Public Policy, IAB Europe
(matthiesen@iabeurope.eu)

iab europe interactive advertising bureau

Technical standard in development and may be subject to changes.

Presentation updated 7 Dec, 2017