Last Chance to fix eIDAS: Secret EU law threatens Internet security

Update: 13 days before the first eIDAS vote, still no public text

2nd November 2023

After years of legislative process, the near-final text of the eIDAS regulation has been agreed by trialogue negotiators[1] representing EU's key bodies and will be presented to the public and parliament for a rubber stamp before the end of the year. New legislative articles, introduced in recent closed-door meetings and not yet public, envision that all web browsers distributed in Europe will be required to trust the certificate authorities and cryptographic keys selected by EU governments.

These changes radically expand the capability of EU governments to surveil their citizens by ensuring cryptographic keys under government control can be used to intercept encrypted web traffic across the EU. Any EU member state has the ability to designate cryptographic keys for distribution in web browsers and browsers are forbidden from revoking trust in these keys without government permission.

This enables the government of any EU member state to issue website certificates for interception and surveillance which can be used against every EU citizen, even those not resident in or connected to the issuing member state. There is no independent check or balance on the decisions made by member states with respect to the keys they authorize and the use they put them to. This is particularly troubling given that adherence to the rule of law has not been uniform across all member states, with documented instances of coercion by secret police for political purposes.

The text goes on to ban browsers from applying security checks to these EU keys and certificates except those pre-approved by the EU's IT standards body - ETSI. This rigid structure would be problematic with any entity, but government-controlled standard bodies are especially susceptible to misaligned incentives in cryptography. ETSI in particular has both a concerning track record (1,2,3) of producing compromised cryptographic standards and a working group dedicated entirely to developing interception technology.

The introduction of this text so late in the legislative process and behind closed doors is also deeply concerning for democratic norms in Europe. Although the deal itself was publicly announced in late June, the announcement doesn't even mention website certificates, let alone these new provisions. This has made it extremely difficult for

civil society, academics and the general public to scrutinize or even be aware of the laws their representatives have signed off on in private meetings.

Outcry across academia, civil society and industry

Over 500 cyber security experts and researchers from around the world have signed an open letter calling on the EU to abandon these plans and safeguard the web:

> After reading the near-final text, we are deeply concerned by the proposed text for Article 45. The current proposal radically expands the ability of governments to surveil both their own citizens and residents across the EU by providing them with the technical means to intercept encrypted web traffic, as well as undermining the existing oversight mechanisms relied on by European citizens.
> […]
> We ask that you urgently reconsider this text and make clear that Article 45 will not interfere with trust decisions around the cryptographic keys and certificates used to secure web traffic.

Civil society groups have also backed the letter, including the Internet Society, European Digital Rights (EDRi), the EFF, Epicenter.works and many more.

Their calls have also been echoed by companies that help build and secure the Internet including the Linux Foundation, Mullvad, DNS0.EU and Mozilla who have put out their own statement.

What next?

This text is subject to approval in the final closed-door trialogue meeting in Brussels on November 8th, after which it will be published and presented for formal ratification in the European Parliament. This is expected to be in the first few months of 2024, but this vote is seen as a formality with the text of trialogue negotiations typically being adopted into law without alteration.

If you're a European citizen, you can write to the member of the European Parliament responsible for the eIDAS file - Romana JERKOVIĆ - and register your concern.

If you're a cybersecurity expert, researcher or represent an NGO, consider signing the open letter at https://eidas-open-letter.org.

Read More

- How does Article 45 enable the interception of web traffic?
- The open letter by cybersecurity experts, scientists and researchers
- The open letter by industry

Coverage around the web

European Press

- 🇦🇹 Der Standard: Forschende warnen vor möglicher Netzüberwachung durch digitale ID

- 🇧🇪 DataNews: Wettekst Europese digitale identiteit kan encryptie en privacy onderuit halen
- 🇧🇪 Het Belang van Limburg: Honderden wetenschappers luiden alarmklok over nieuwe EU-wetgeving die digitale veiligheid ondermijnt
- 🇧🇪 Le Soir (paywall): Gare au risque de surveillance généralisée du Web en Europe, disent des chercheurs en sécurité
- 🇩🇪 netzpolitik.org: Hunderte Wissenschaftler:innen und dutzende NGOs warnen vor Massenüberwachung
- 🇩🇪 Der Tagesspiegel (paywall): Digitale Identitäten: Expert:innen warnen vor EU-Wallet
- 🇫🇷 BFM: “Surveiller ses citoyens”: des spécialistes alertent contre un texte européen visant les navigateurs Web
- 🇫🇷 Le Monde: Inquiétudes autour d’un règlement européen sur la sécurité des navigateurs Web
- 🇫🇷 01.net: Des chercheurs et ONG vent debout contre une loi européenne qui permettrait de « surveiller le trafic Internet de n’importe quel citoyen européen
- 🇫🇷 Developpez: Dernière chance de corriger eIDAS : la loi secrète de l’Union européenne sur l’identification électronique qui menace la sécurité de l’internet
- 🇫🇷 NextInpact: Les navigateurs web devront-ils accepter les certificats de sécurité imposés par les autorités ?
- 🇫🇮 AfterDawn: EU:n lakiesitys mahdollistaisi EU-maille kansalaisten selainten salakuuntelun
- 🇬🇷 iGuRu: ΕΕ κανονισμός eIDAS: Ο διάβολος βρίσκεται στη λεπτομέρεια
- 🇮🇹 Key4biz : eIDAS 2.0, insicurezza by design?
- 🇮🇹 iLSoftware: eIDAS, i certificati europei potrebbero rendere insicure le comunicazioni
- 🇳🇱 AG Connect: Honderden security-experts slaan alarm over EU-plan waarmee alle internetverkeer valt te onderscheppen
- 🇳🇱 Security.nl: Internetbedrijven slaan alarm over certificaatplan Europese digitale identiteit
- 🇳🇱 Dutch IT Channel: Zorgen over Euroepese eIDAS regelgeving
- 🇳🇱 AD: Cyberdeskundigen in rep en roer om ‘gevaarlijke’ EU-wet: ‘We duiken de afgrond in’
- 🇵🇱 Sekurak: Wg nowej propozycji prawa EU, rządy będą mogły wystawiać certyfikaty TLS dla serwisów webowych. A przeglądarki będą musiały to akceptować. Gigantyczne możliwości podsłuchu.
- 🇨🇭 Inside IT: EU vereinfacht Überwachung von Bürgerinnen und Bürgern
- 🇸🇪 Femte Juli: Nu tar EU kontrollen över din web-läsare
- 🇪🇪 Zone: Ootamatu oht privaatsusele ja vabadusele Internetis

English-language Press

- The Record: EU urged to drop new law that could allow member states to intercept and decrypt global web traffic
- Techdirt: EU Tries To Slip In New Powers To Intercept Encrypted Web Traffic Without Anyone Noticing
- Politico (paywall): EIDAS WARNING
- Biometric Update: Hold up: 300 say eIDAS rules could make surveillance easier for EU nations
- Hackaday: Proposed European Electronic ID Law Raises Concerns
- StackDiary: Mozilla and others warn EU identity cert rules undermine security
- Computer Weekly: EU digital ID reforms should be ‘actively resisted’, say experts

Statements by Companies, Organisations and Individuals

- Patrick Breyer, Pirate Party MEP: The reform is almost through, last round of negotiations on Wednesday. A massive storm of protest is needed…
- Alec Muffett: Hot on the heels of #ChatControl and in the name of “identity” and “consumer choice” the EU seeks the ability to undetectably spy on HTTPS communication
- Open Source Security Foundation: OpenSSF Co-Signs Industry Joint Statement on Article 45 in the EU’s eIDAS Regulation
- Mullvad: EU Digital Identity framework (eIDAS) another kind of chat control?
- Internet Society: Civil Society Experts Voice Concern as New EU Digital Identity Regulation Finalized
- Tutanota: Say NO to broken browsers!
- Matrix.org Foundation: Sounding the alarm about the EU’s proposed eIDAS reform.
- Google: We urge lawmakers to heed the calls of scientists and security experts to revise this part of the legislation
- Scott Helme: What the QWAC?!
- EFF: Article 45 Will Roll Back Web Security by 12 Years

Online Discussions

- Hacker News
- Lobste.rs
- Reddit’s r/privacy
- Mark Nottingham on TechPolicy Mastodon

1. Wayback Machine ↩