

EU Policies Meet Global Practices

The Discourse on Qualified Website Authentication Certificates (QWAC)

**Johannes
SEDLMEIR**

Acting Professor
University of Münster
Germany



**Pol
HÖLZMER**

Doctoral Researcher
University of Luxembourg, SnT
Luxembourg



Introduction



Source: <https://securityriskahead.eu> (Mozilla, 2023)

About Us: QWAC controversy Phase 3



What Changed: Not much actually. Or... actually, a lot?

Draft Article 45 (leaked version)

“[QWACs] [...] shall be recognised by providers of web-browsers.”

“Providers of web-browsers shall recognise and display the information [...] in a user-friendly manner.”

“Providers of web-browsers shall not impose, for the purposes of recognition and display of [QWAC], [additional] requirements [...]”

“The requirements laid down in Annex IV shall be considered both necessary and sufficient to ensure the highest possible level of security for [QWAC].”

until 2019

http://unsecure-domain.com

 Secure | <https://domain-validation.com>

 Evil Corp Inc. [US] | <https://extended-validation.com>

after 2019

 Not Secure | <http://unsecure-domain.com>

 <https://domain-validation.com>

 <https://extended-validation.com>

after 2025?

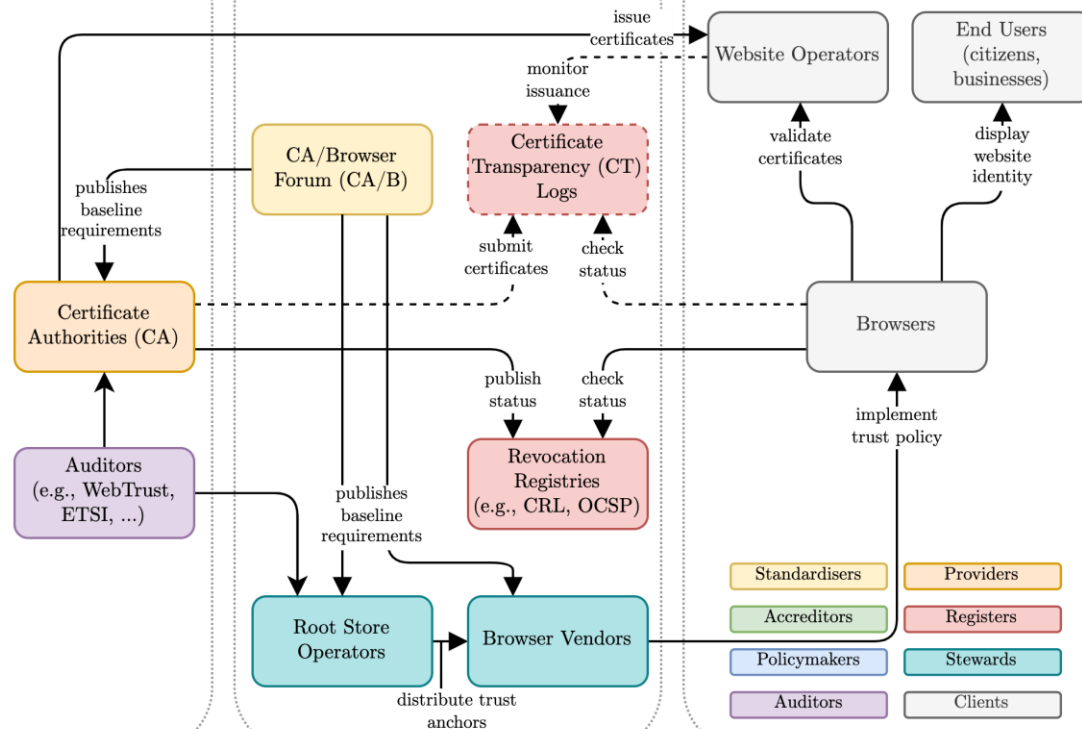
 European Gov. [EU] | <https://qualified-web-authn.eu>

Ecosystem: The WebPKI

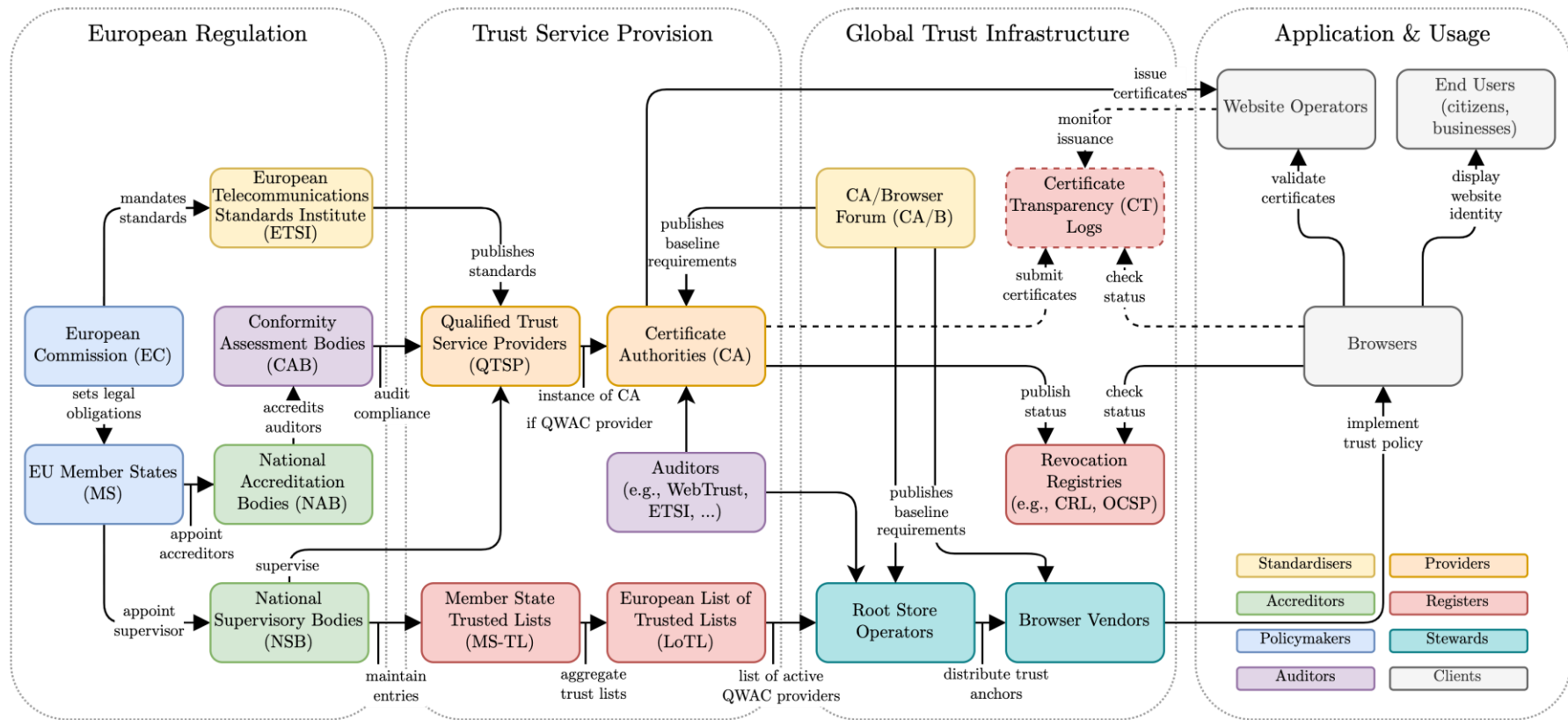
Trust Service Provision

Global Trust Infrastructure

Application & Usage



Ecosystem: The WebPKI and eIDAS



Research Design

Multivocal Literature Review

- ☐ Academic Papers (n = 4)
(Entschew et al., 2022, 2024; Martius et al., 2024; Wazan et al., 2024)
- ☐ Legal Documents and Reports (n = 30)
(e.g., EU Parliament, EU Commission, and EU Council)
- ☐ Technical Reports, Products, and Presentations (n = 30)
(e.g., ENISA, ETSI, EU Commission, Trust Service Forum, EnTrust)
- ☐ Supporter/Critics' Position Papers (n = 14; m = 26)
(e.g., European Signature Dialog, Bitkom) / (e.g., Mozilla, CA/B Forum, EFF)
- ☐ Media Reports and Blog Posts (n = 32)
(e.g., Feisty Duck, Twitter, LinkedIn)

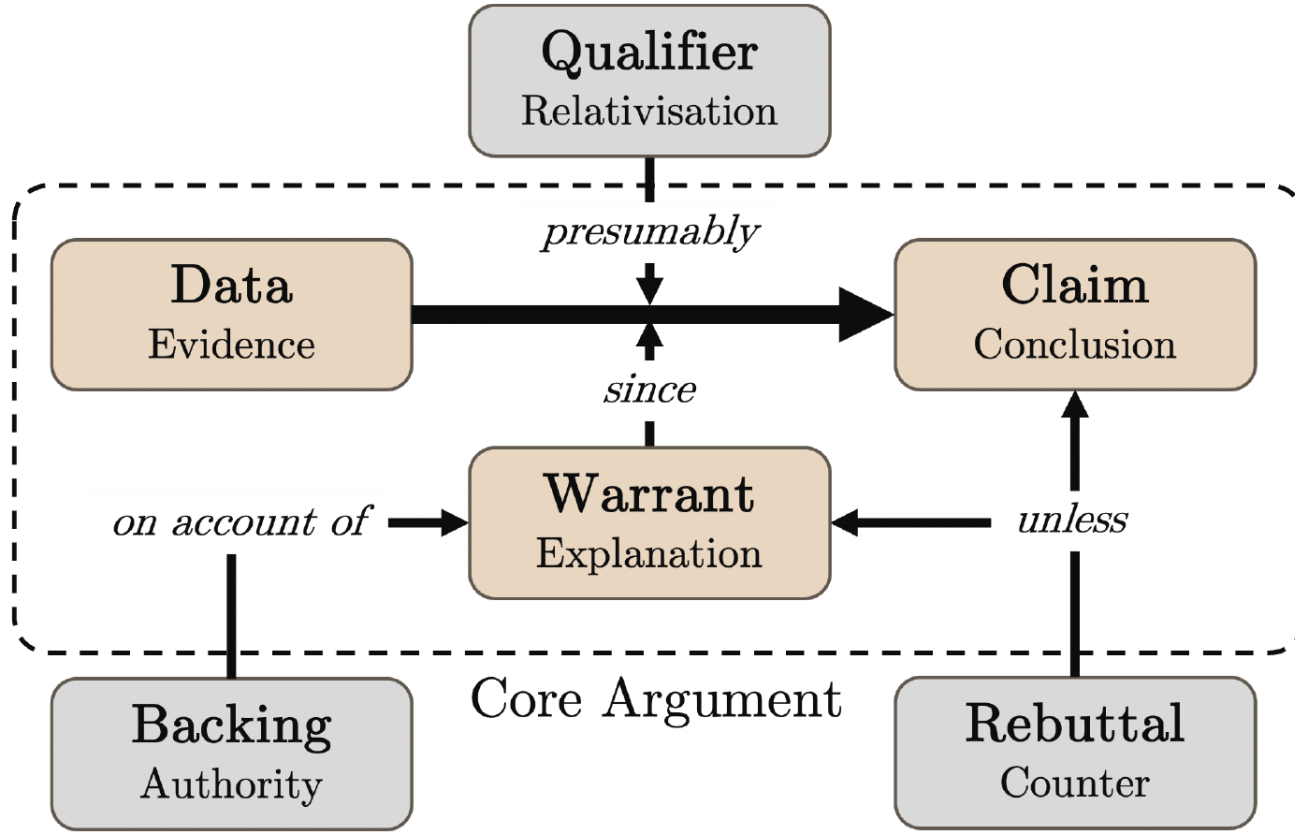
Semi-structured Interviews

- ☐ **Stance:** 6x Supporter, 4x Neutral, 5x Critic
- ☐ **Domain:** 6x Academia, 2x Government, 1x Industry, 1x Regulatory, 1x Standards

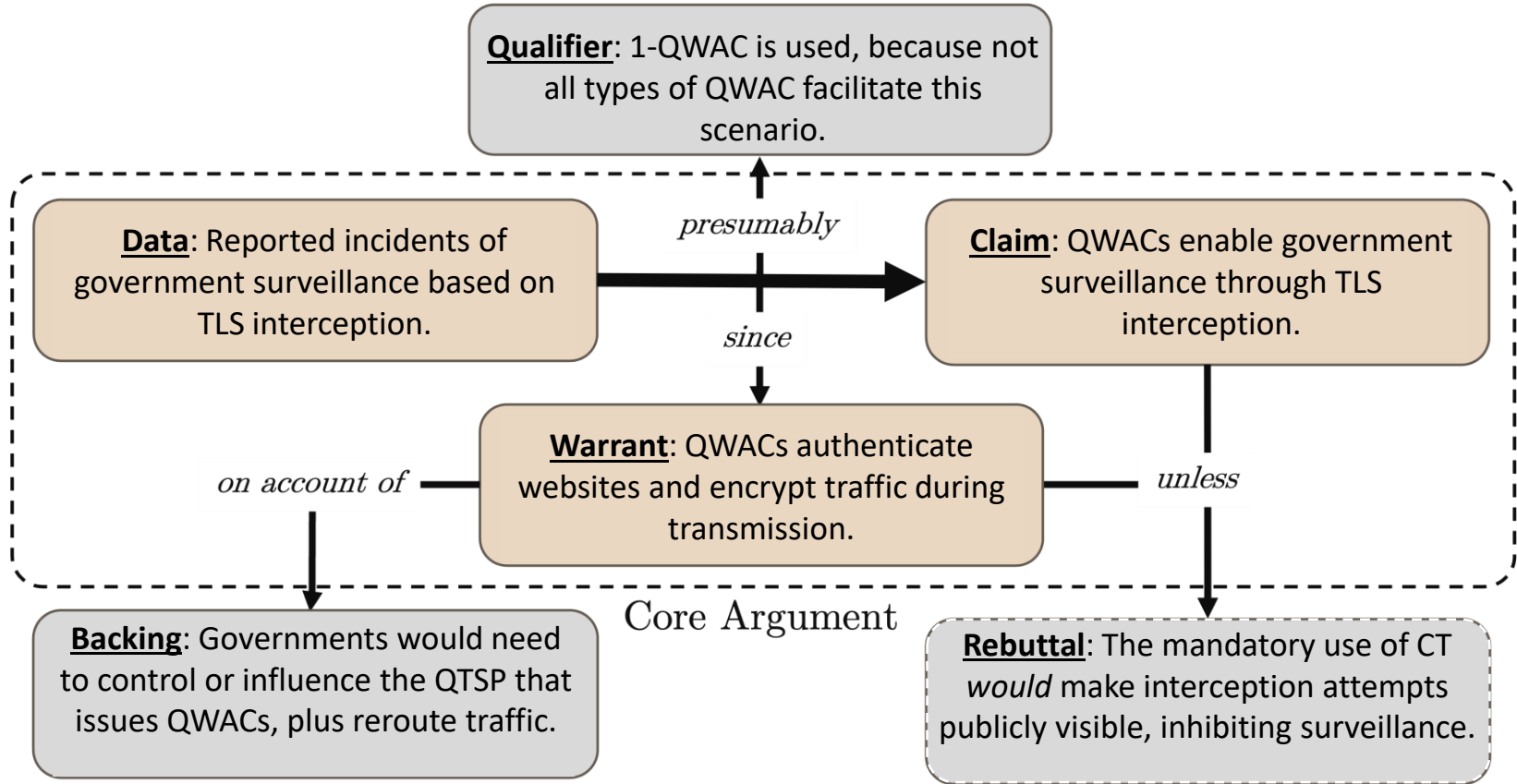
Argument Evaluation

- ☐ **Toulmin Model:** 1247 components, 20 arguments

Toulmin Model: In a nutshell



Toulmin Model: In a nutshell



Dimensions of the Discourse

Argument Classes Means & End

Security & Trust

Governance & Sovereignty

Compliance & Interoperability

Theoretical Lens

Socio-Technical

Institutional

Technical

Information
System

Security & Trust

[ST-S1] **QWACs strengthen Website Identity Assurance** by binding a supervised legal-entity identity to a TLS endpoint through harmonized ETSI specifications.

[ST-S2] **QWACs display a Transparent Trust Indicator** by mandating that browsers provide verified identity fields in a user-friendly manner.

[ST-S3] **QWACs protect Users from Fraudulent Websites** by exposing vetted legal names and jurisdictions that can be compared to brand claims at connection time.

[ST-C1] **QWACs do Not Enhance User Risk Awareness** because humans don't adapt behavior by certificate cues, and removing EV indicators didn't reduce overall security.

[ST-C2] **QWACs do Not Deliver Effective Trust Signals** because certificate identity cues themselves are too weak to influence reliable decisions by untrained users.

[ST-C3] **QWACs degrade User Data Protection** by introducing potential metadata leakage through additional lookups or validation steps, especially with 2-QWAC.

[ST-C4] **QWACs introduce New Attack Vectors** by introducing additional verification logic and mandated UI elements, increasing complexity and the risk of user over-trust.

Governance & Sovereignty

[GS-S1] **QWACs promote Fair Competition in Digital Markets** by creating a statutory path for QTSPs to be recognized in browsers via MS-TL and LoTL listings.

[GS-S2] **QWACs strengthen EU Digital Sovereignty** by embedding organizational authentication into EU-supervised trust frameworks.

[GS-S3] **QWACs advance the EU Digital Single Market** by harmonizing recognition and display of identity across borders.

[GS-C1] **QWACs facilitate Government Surveillance** because state-controlled QTSPs could issue interception certificates that must be accepted until detected.

[GS-C2] **QWACs undermine Neutral Global Trust Models** because mandatory legal recognition constrains browser discretion and may conflict with CA/B Forum norms.

[GS-C3] **QWACs conflict with Existing Root Store Standards** by shifting trust anchor criteria from browser policy to statutory listings.

Compliance & Interoperability

[CI-S1] **QWACs integrate Website Authentication into EU Trust Schemes** by standardizing identity validation under ETSI supervision and MS-TL/LoTL governance.

[CI-S2] **QWACs integrate with EU Cybersecurity Directives** by aligning with ENISA recommendations and NIS2-related governance.

[CI-S3] **QWACs strengthen Accountability and Transparency** by surfacing legally verified identities at the point of interaction, consistent with GDPR principles.

[CI-C1] **QWACs create Fragmented Trust Ecosystems** because 2-QWAC bindings require extra discovery and status checks not covered by existing automation.

[CI-C2] **QWACs undermine Technological Neutrality Principles** by privileging one artifact and narrowing space for alternative solutions.

[CI-C3] **QWACs increase Complexity and Costs for Website Operators** by requiring dual audits and new verification tooling for operators

[CI-C4] **QWACs underperform Compared to Existing Measures** because DV, CT logging, and short lifetimes already provide efficient safeguards.

Our Recommendations

Three main lessons

- ☐ **Security & trust**
Where identity is consumed matters more (i.e. user acceptance) than how it is issued.
- ☐ **Governance & Sovereignty**
Leave no room for misuse of authority and ensure global interoperability.
- ☐ **Compliance & Interoperability**
Will come from CT logs rather than from accreditation and certifications.

Actionable insights

- ☐ **Browsers** should define a standardized and minimal identity interface.
- ☐ **Providers** should log issuance in CT and use privacy-preserving revocation.
- ☐ **Regulators** should fund reference tools, and cross-browser UX guidelines.
- ☐ **Relying parties** should pilot QWACs where legal identity matters.

Conclusion

There are still many uncertainties that complicate a final assessment of the controversy.

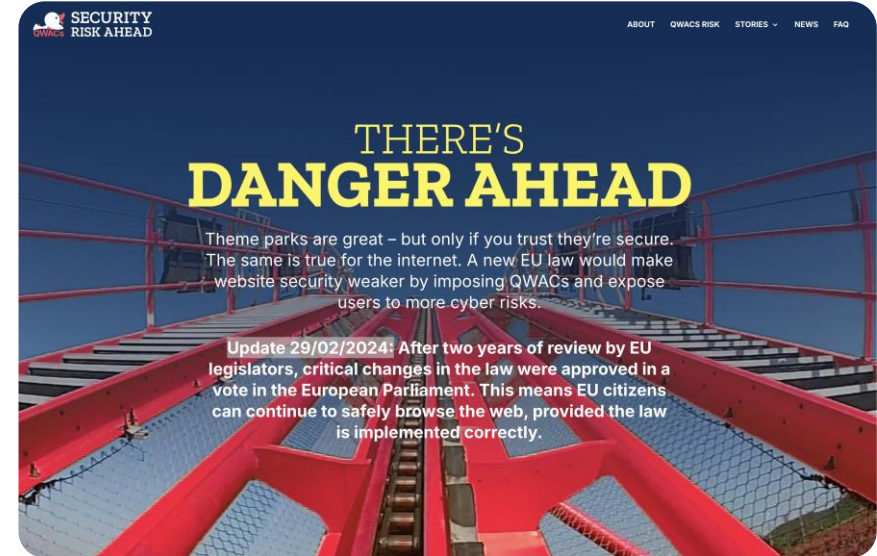
- ➔ Was the political capital spent worth it?
- ➔ Are there substantial sovereignty improvements?

Further ideas for future research:

- ☐ Compare discourse to other incidents involving disinformation
- ☐ Behavioural studies on the effectiveness of different trust indicators and training
- ☐ Recommendations for stakeholders (e.g., scientists) on how to navigate such discourses

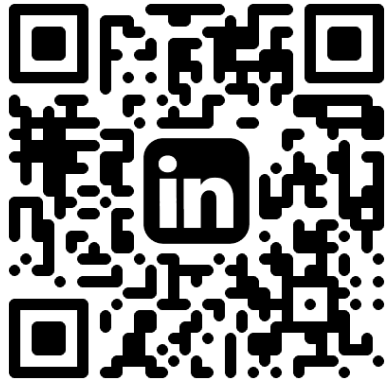
Stay tuned for the preprint

- ☐ If you feel there is something important we should know, please approach us.
- ☐ If you would like to be notified of the publication, please also contact us.



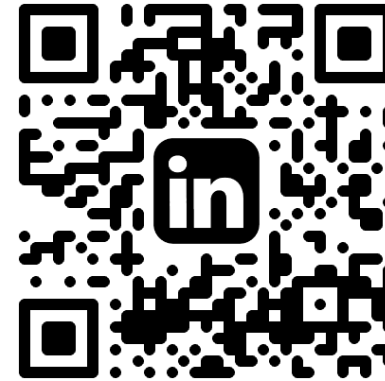
Johannes SEDLMEIR

johannes.sedlmeir
@uni-muenster.de



Pol Hölzmer

pol.hoelzmer
@uni.lu



This research was supported in part by Luxembourg's Ministry for Digitalisation, PayPal, and the Luxembourg National Research Fund (FNR) (P17/IS/13342933/PayPalFNR/Chair in DFS/Gilbert Fridgen)).

