# eIDAS 2, ARTICLE 45
# WHERE WE ARE, AND POSSIBLE OUTCOMES

**Chris Bailey**

VP Strategy and Business Development, Entrust

ENISA Trust Services Forum - 28 October 2022 - Berlin

ENTRUST

SECURING A WORLD IN MOTION

# WHERE ARE WE, AND HOW DID WE GET HERE?

# PROGRESS OF EIDAS 2 LEGISLATION (ARTICLE 45)

- **EU Commission** in strong support of original proposal
- **EU Council** supports Commission proposal
  - Some Council members want to strengthen it
- Amendments considered in **EU Parliament**
  - Lead committee votes late November
- **Trialogue** to start in January 2023
- Final **plenary vote** is expected in Summer 2023



ENTRUST

# THE "RIGHT TO KNOW" IS WELL ESTABLISHED

- "… a **provider must supply [its identity]** … **in a clear and unambiguous manner**, … before conclusion of the contract or, … **before the service is provided**"

  *^ Directive 2006/123/EC Services in the internal market*

- "Before the consumer is bound by a contract … **the trader shall provide the consumer** … **the identity of the trader** ... in a clear and comprehensible manner".

  *^ 2011/83/EU Directive on consumers rights*

- **GDPR requires providing "controller" identity** (i.e., website owner information) **to the "data subject"** (i.e., website visitor) when personal data is collected "… **in a concise, transparent, intelligible and easily accessible form** …"

  *^ Regulation (EU) 2016/679 (GDPR)*

- **"**[T]o **allow consumers** and all other interested parties to **know the identity** and reliability of a company and have full access to the **most relevant information concerning a company**, Member States are bound by article 14 of *Directive* 2017/1132/EU".

  *^ Impact assessment report eIDAS revision*



ENTRUST

# BROWSER NON-RECOGNITION OF QWACs

**2021 Impact Assessment Report *findings*:**

- "QWACS have been created by the eIDAS **Regulation to enforce EU rules on a 'right to know'** regarding the identity of websites" as regulated by 2011/83/EU Directive on consumers rights
- "The *lack of recognition of QWACs* by web-browsers ***may also conflict with the protection of fundamental rights of consumers*** as enshrined in the Treaty on the Functioning of the European Union"
- **"[W]eb browsers refuse to include [QWAC root CAs] in their root stores** and to display [QWACs] clearly, which **makes these certificates *unusable*** for traders and consumers. ***Although the Commission initiated a dialogue in 2018 to promote implementation of QWACs in the browser environment,* web-browsers continue to refuse supporting QWACs and have been unable to present alternatives with the same degree of legal assurance."**



ENTRUST

# OPPOSITION TO ARTICLE 45

- **Why do some browsers oppose?**
  - *Issue 1:* Some browsers believe that displaying identity has limited value
    - But *Microsoft*: "Another part of this provision [eIDAS 2] entails modifying the browser UI to display certain information to the user. Microsoft also **understands the valid concerns behind this requirement**, aiming at providing a better online framework where the users can have visible indicators, and we are willing to accommodate such demands."
      *Source: Microsoft Position Paper – June 2022*
  - *Issue 2:* Some browsers want FULL control over their root store
- **What's to be done?**
  - *Issue 1:* EU Council / Commission stand firm behind Article 45. Will *not* back away from "Right to Know", through a "user-friendly" UI, because it is already the law.
  - *Issue 2:* Possible compromise on trust of QTSPs



ENTRUST

# **ISSUE 1**
# USER-FRIENDLY USER INTERFACE (UI)

ENTRUST

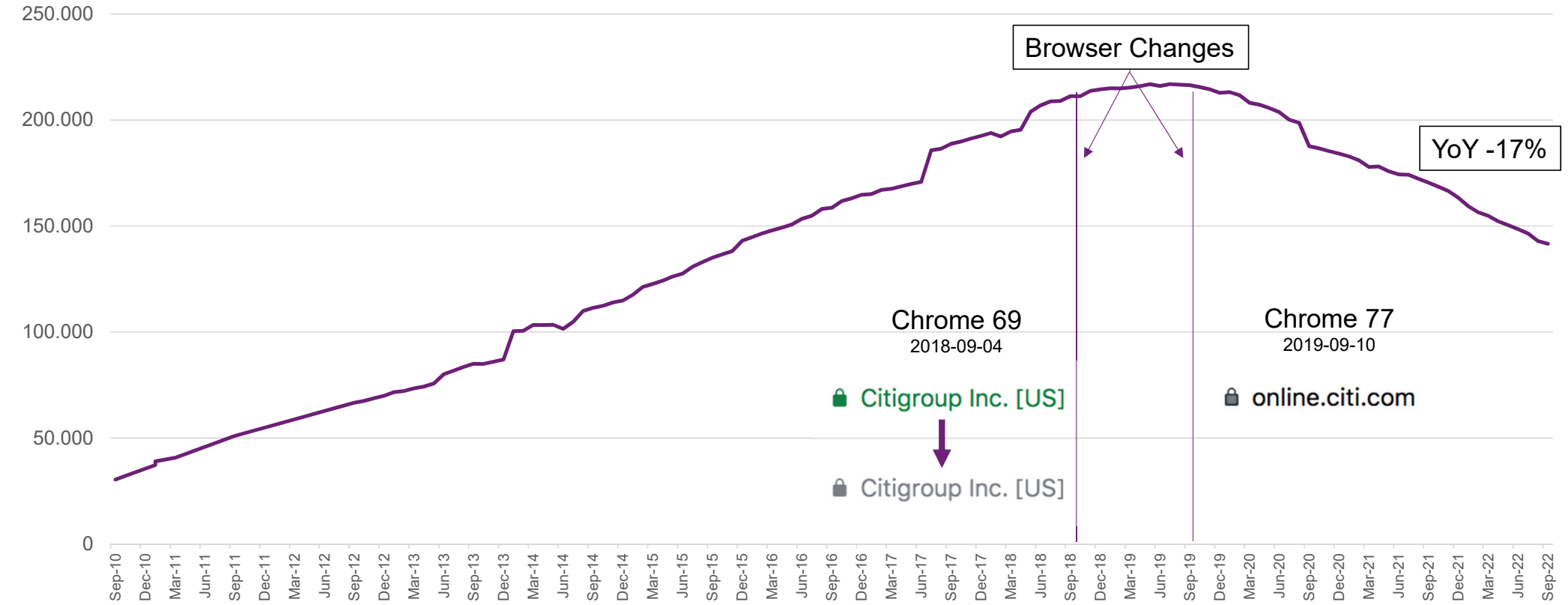
# EV HAD FLAWS

- **Lack of user awareness**, caused by the inability to educate users with a consistent message:
  - Non-standardized display across browsers
  - Not shown on all devices
  - Too frequent changes to the UI design (can't educate with constant changes)
- **Identified UI problems were never resolved**
  - Conflicting Indicators (e.g., use of indicators stating 'secure' or 'trusted' for DV certificates)
  - Need *more* than country indicator to fully disambiguate organizations
  - Identity information not always displayed (e.g., pop-up windows)
- **Even with these issues, EV adoption growing each year**
  - Since proactive EV UI was removed, it is declining -17% a year

**How do we fix this?**

ENTRUST

# -17% / yr EV DROP SINCE PROACTIVE UI REMOVED




ENTRUST

# ELEMENTS OF A SUCCESSFUL IDENTITY UI

- It must be proactive, distinguish and always display the entity behind the website
- It must be simple, and easy for users to understand
- It must be easy for users to obtain further website identity information if they want it
- It must work equally well in mobile, tablet, and desktop environments with a variety of displays and font sizes
- The information shown must have a single purpose and only include information which is based on a minimal level of trustworthiness and independent verification
- It must be easy to explain through user education, and browsers, CAs, and governments must cooperate on a program of user education
- It must be substantially common and consistent across all browsers



ENTRUST

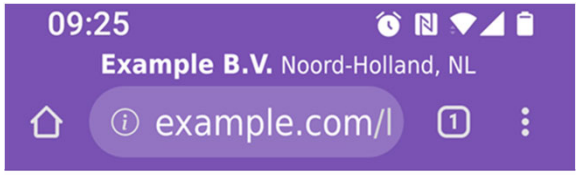
# DO YOU REMEMBER OUR CA DAY PRESENTATION FROM LAST YEAR?

https://bit.ly/3rTi96b

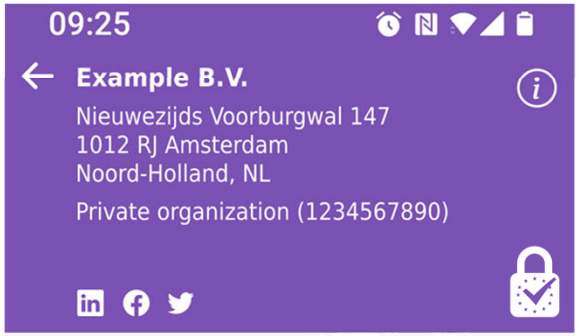
ENTRUST

# VERIFIED IDENTITY

## QWAC / EV - IDENTITY CERTIFICATE




**With or without** asking for user data




**Identity details** shown after clicking symbol or identity summary above address bar

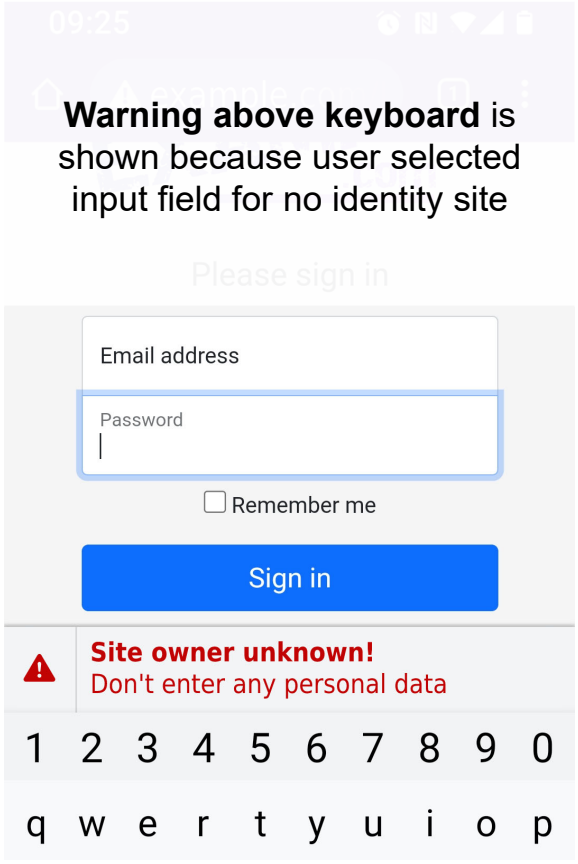

**Sticky identity summary** shown on top of screen when scrolling down on the page

ENTRUST

# DATA ENTRY INTERFACES

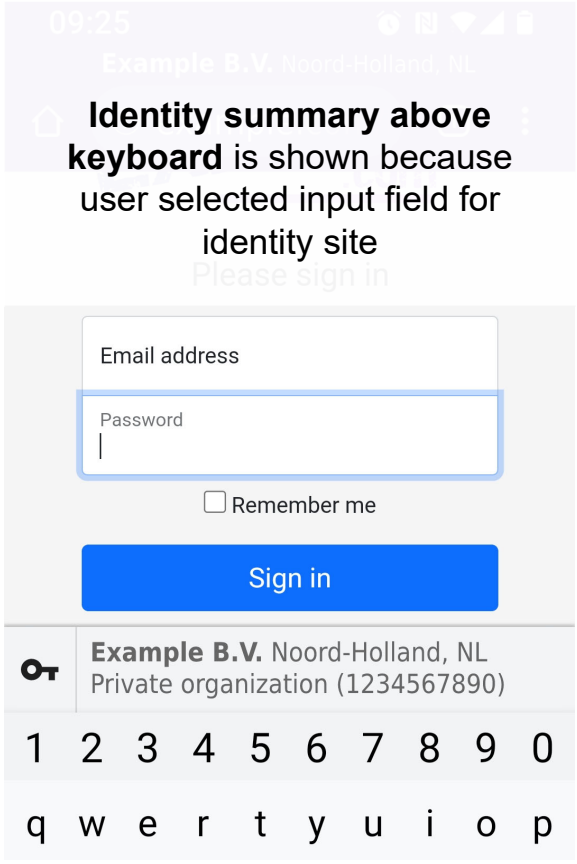
## NO IDENTITY

**Warning above keyboard** is shown because user selected input field for no identity site

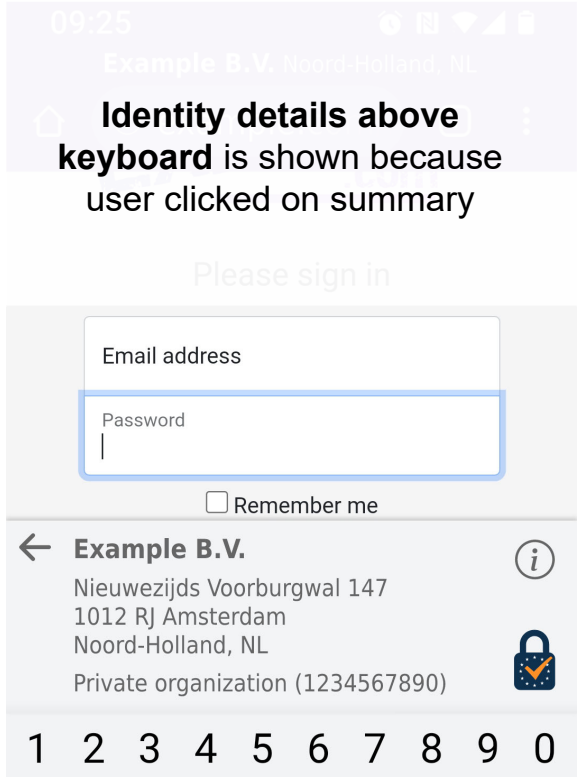



## QWAC / EV IDENTITY

**Identity summary above keyboard** is shown because user selected input field for identity site




**Identity details above keyboard** is shown because user clicked on summary






ENTRUST

# ISSUE 1: USER-FRIENDLY IDENTITY UI

**An approach to establishing user-friendly identity UI:**

- Establish a special task force of stakeholders (incl. EU Commission, Browsers, QTSPs)
  - Develop a policy/criteria for a user-friendly identity user interface (as discussed in ”Elements of a Successful UI” slide)
  - Develop a wireframe (blueprint design) of the identity user interface including its position, components and interactions
  - Develop criteria based on the EU objective to measure the user-awareness and effectiveness of the user interface
- Continue improving, using both infrequent and subtle changes

**Comment:** We have never had a standard for the identity UI



ENTRUST

# ISSUE 2
# BROWSER TRUST OF QTSPs

ENTRUST

# ISSUE 2: BROWSER TRUST OF QTSPs

**Possible solution:**

- Allow immediate browser distrust of individual bad QWACs, notification to QTSP and EU with justification and post evaluation
- Create a transparent process for browser distrust of QTSPs with involvement by EU, Supervisory Body, auditor, and QTSP
  - Create severity levels – *low, medium, high, urgent* – with SLAs to avoid delay
  - Allow remediation opportunities for most cases, monitoring
  - Role for neutral party as final decider – see EU Parliament ITRE Amendments 246, 553, 584, 585

**Comment:** Result is cooperative model created by the EU



ENTRUST

# **ISSUE 3**
# CONFLICTING STANDARDS

ENTRUST

# ISSUE 3: CONFLICTING "STANDARDS BODIES"

**Possible solution:**

- Browsers bring all extra browser rules for consensus and approval under the CA/Browser Forum for industry standards which are audited under ETSI and WebTrust
- ETSI and CA/Browser Forum
  - work together to harmonize all requirements, *so long as there are no conflicts*
  - each can add additional requirements, *so long as there are no conflicts*

**Comment**: You can't have multiple trust schemes if they conflict (ETSI, CA/B Forum, Microsoft, Mozilla, Chrome, Apple, etc…)



ENTRUST

# WHAT TO DO NEXT?

- Establish agreement on the elements of a successful UI
- Start special EU task force of stakeholders to work on user interface policy, design and criteria to measure user-awareness and effectiveness to the spirit of the regulation
- Start work on public process to review distrust of QTSPs and individual QWACs that includes the EU Commission, Supervisory Bodies, auditors (ACAB'c), QTSPs and a neutral party as final decider
- Bring browser root program rules to CA/Browser Forum for consensus and approval
- ETSI and CA/Browser Forum to harmonize requirements



ENTRUST

# THANK YOU!
# QUESTIONS?

**Chris Bailey**

chris.bailey@entrust.com

ENTRUST