

DESIGNING THE NEW eIDAS 2 BROWSER UI

Chris Bailey, Entrust

September 2021 - CA Day



ENTRUST

SECURING A WORLD IN MOTION

What does eIDAS 2 require?

“[Browsers] should recognise and display [QWACs] to provide a high level of assurance, allowing website owners to assert their identity as owners of a website and users to identify the website owners with a high degree of certainty.”

“[QWACs] *** shall be recognised by web-browsers. For those purposes web-browsers shall ensure that the identity data provided *** is displayed in a user friendly manner.”

Web-browsers shall ensure support and interoperability with [QWACs] ***”

What about **GDPR** and **website identity**?

Recital (39): Any processing of personal data should be lawful and fair. It should be transparent to natural persons ^{***}. The principle of transparency ^{***} concerns, in particular, information to the data subjects on the identity of the controller

Recital (42): ^{***} [T]he controller should be able to demonstrate that the data subject has given consent to the processing operation.^{***} For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended.



What about **GDPR** and **website identity**?

Article 4 – Definitions:

‘Personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, [or] an online identifier

Article 13 – Information to be provided where personal data are collected from the data subject:

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: (a) the identity and the contact details of the controller ***

GDPR requires website identity



- › **GDPR requires websites** who ask EU consumers for personal data to show the **identity of the data controller**
- › eIDAS 2 enables users to **identify website owners with a high degree of certainty** in a user-friendly (consistent) manner
- › It's a **GDPR challenge for non-identity websites (DV)** to **comply with the regulation** when allowing consumers to provide personal data

A Brief History of EU Identity Requirements



- › Providing “controller” identity to the “data subject” “in a clear and unambiguous manner” and “before conclusion of contract or services” dates back to 1997 and enforced by multiple directives such as:
- › The directive on consumer rights (97/7/EC article 6)
- › The directive on services in the internal market (2006/123/EC article 22).

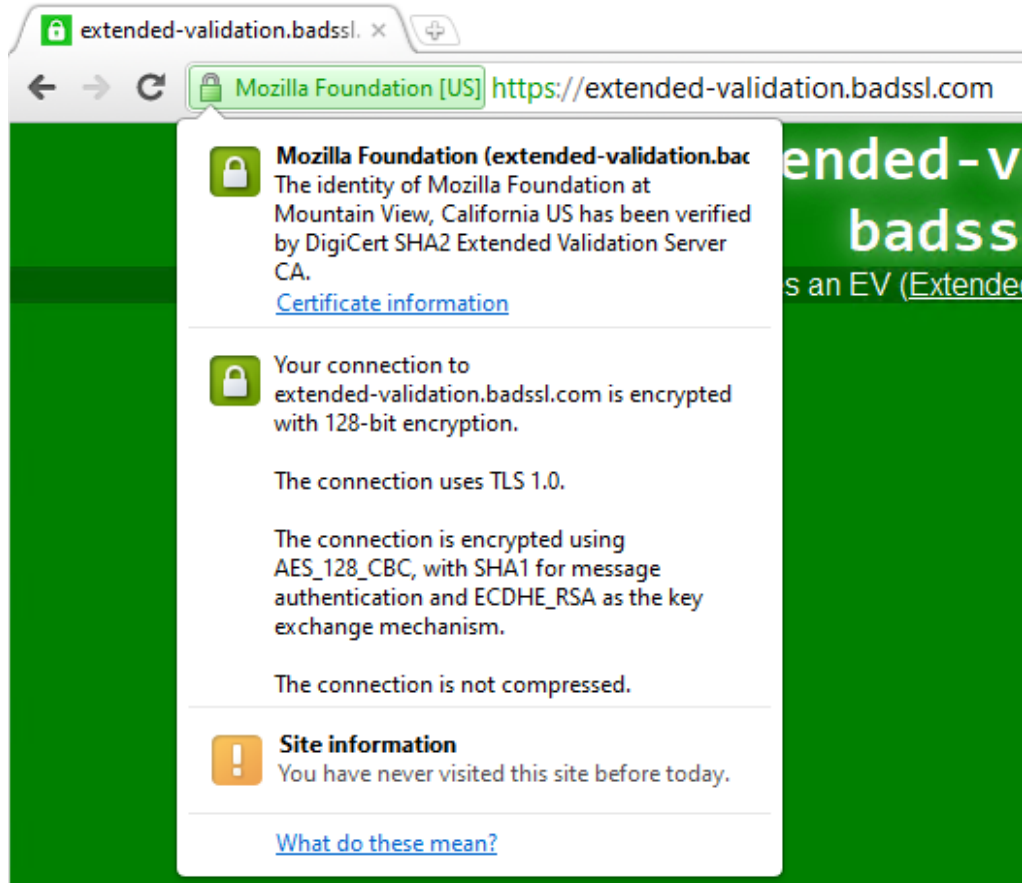
BROWSER HISTORY



ENTRUST

SECURING A WORLD IN MOTION

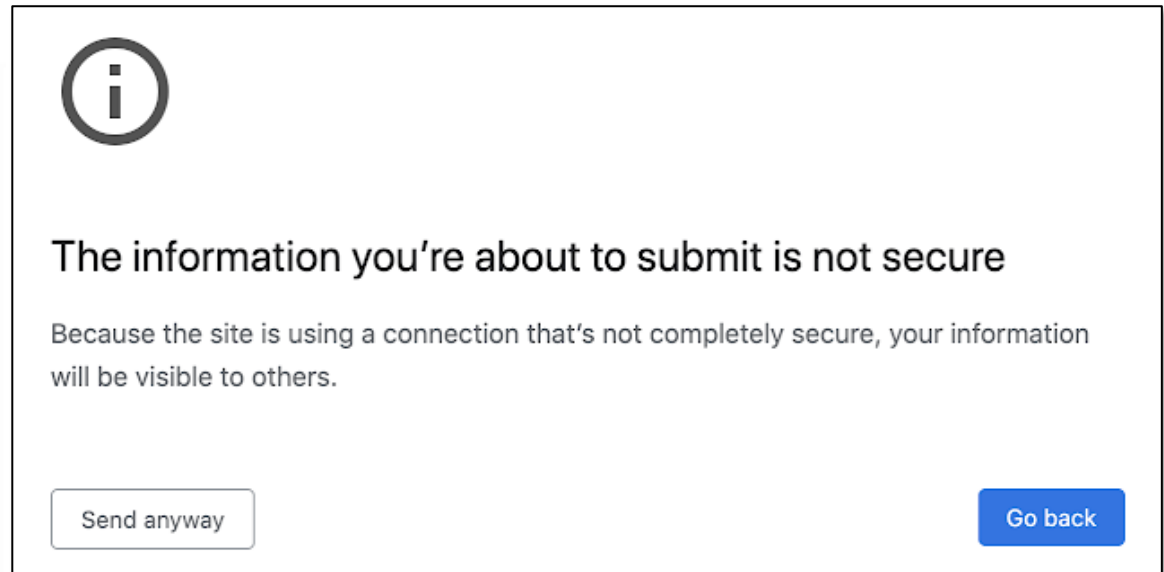
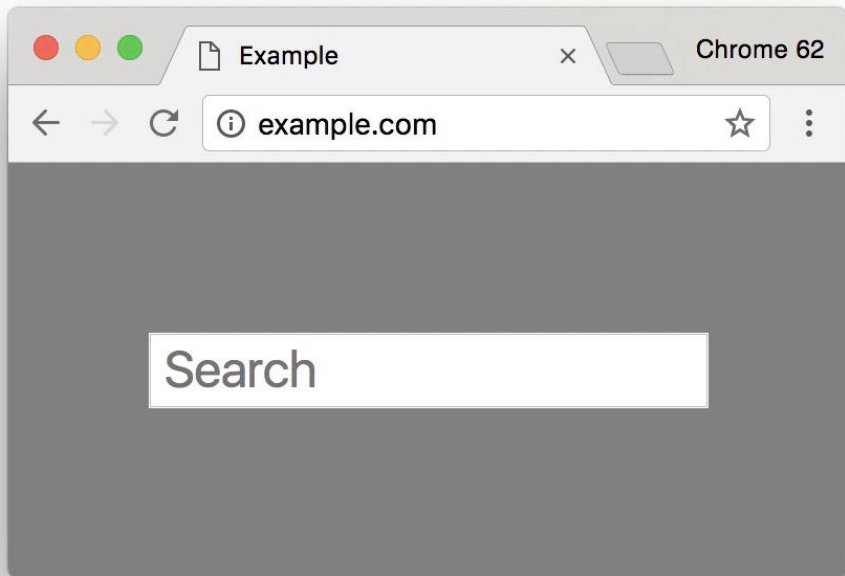
QWACs (and EV) had a browser **identity UI** before



- › **2008** – EV certs introduced. All browsers adopt EV identity
 - Overwhelmed with technical data, still the case today
- › **2014** – EU introduces QWACs, which get EV UI treatment
- › **2017-19** – Browsers gradually remove the proactive QWAC/EV UI
- › **2017-19** – Browsers post warnings for http, sites move to https to avoid warnings

Browsers also showed **warnings** for **user input**

- ▶ When browsers showed UI warnings for http, they also warned users to not type in personal data in fields on or posting to http websites



RETHINKING THE eIDAS 2 QWAC USER INTERFACE



ENTRUST

SECURING A WORLD IN MOTION

Combine new eIDAS 2 UI with user warnings

- ▶ We should re-use both the inform and warning approach for the new QWAC/EV UI
 - Show identity data when available
 - Warn consumers if a non-identity (DV) website asks for personal data
- ▶ This will move legitimate websites to QWACs/EV to avoid the warnings
- ▶ Works in tandem with the new eIDAS 2 identity UI requirement

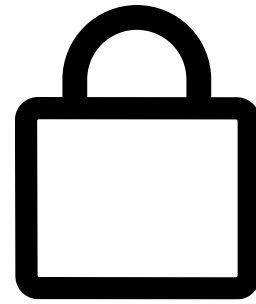
The European Commission should take the lead in designing the new identity UI and warnings to be used by all browsers – and ensure “support and interoperability” for consistency

What are the elements of a **successful identity UI**?

To be successful, a new identity UI must have the following elements:

- It must be simple, and easy for consumers to understand
- It must have a single meaning
- It must be easy for consumers to obtain further website identity information if they want it
- It must be easy to explain through user education, and browsers, CAs, and governments must cooperate on a program of user education
- It must work equally well in mobile, tablet, and desktop environments with a variety of displays and font sizes
- It must be substantially common across all browsers / consistent



First, pick a standard symbol to indicate website identity



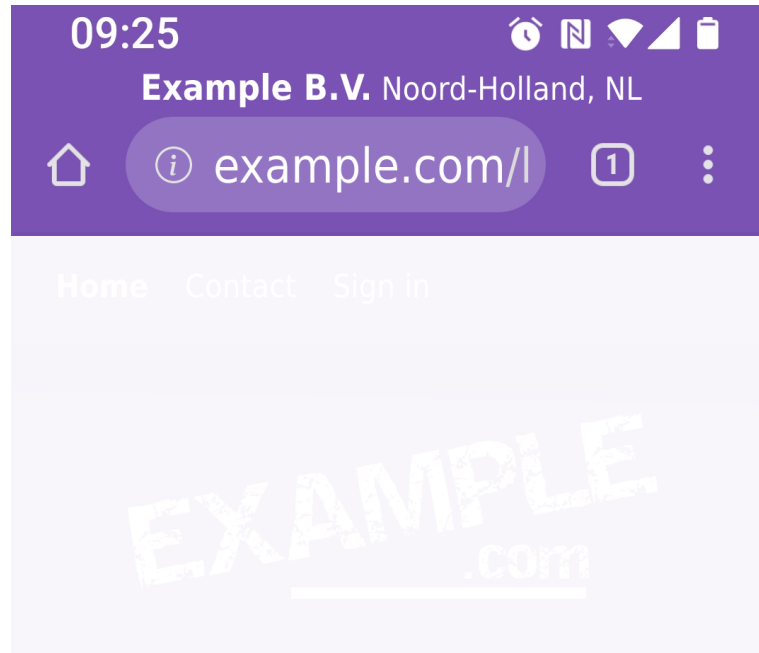
Pick something – **then don't change it or use it for other purposes.** Make the new symbol **standard across browsers** for “interoperability”

Second, pick an *approach* for a new eIDAS UI

- Symbol (“identity” or “no identity”)
 - Compact (good for mobile)
 - Easy to standardize across platforms
 - Easy to teach users
- Proactively show identity name
 - Early confirmation
- Inform and Warn on data entry
 - Minimal education needed
 - More effective
- **A combination of the above**

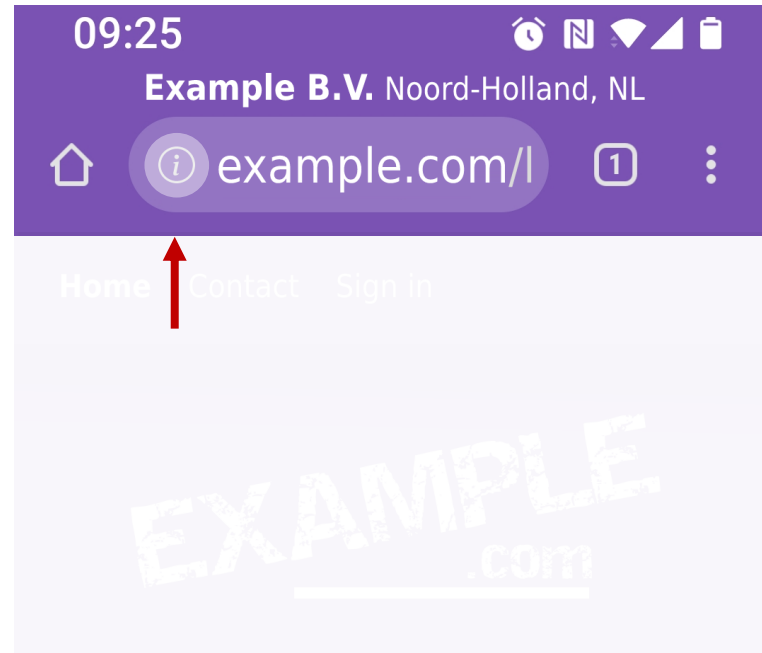
Cert type	UI symbol
QWAC / EV	 (image to indicate identity)
OV and DV	Nothing (encryption is the new normal)
http (unencrypted)	 [Not secure]

Third, require **standard identity view** on symbol click



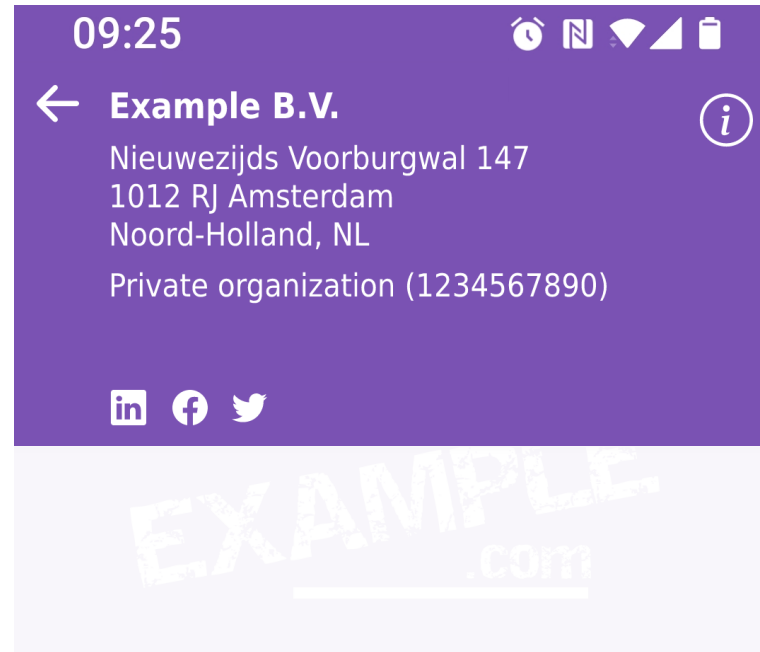
- › **Always show name and location above URL for QWAC/EV**
- › **Identity symbol only** appears in address bar when QWAC/EV identity is present for the website
- › Mobile First Examples
 - Based on Android with the largest font and display size settings
 - These examples can be implemented on all browsers

Third, require **standard identity view** on symbol click



- › Click on the identity symbol to see more identity information (see next slide)

Third, require **standard identity view** on symbol click



All posts Archive Videos Subscribe

Welcome

by Chris Bailey · 22 September 2021

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Curabitur euismod ipsum quis libero feugiat scelerisque. Ut varius, leo nec rhoncus tincidunt, mi nisi rutrum dui, quis vehicula est turpis et nisl. Curabitur lacinia, leo sed vulputate volutpat, mauris justo laoreet nibh, rutrum viverra nulla risus vel magna. Praesent et facilisis dolor. Et ut vestibulum tristique. Etiam pellentesque, arcu tuncit, con

- **Showing detailed identity**
- **Stop showing technical information** to normal users (such as TLS versions, ciphers, etc.)
 - Technical users can get these details through some menu option or in the developer mode.
- Consider adding new verified information (privacy policy, ISO 27701, phone numbers, social media)
- An EU statement or symbol could be shown with the identity details

Third, require **standard identity view** on symbol click

› **The symbol, identity summary and identity details provide a clear and consistent way for users to view the identity information**

- This satisfies several European requirements, including:

- ❖ Consumer rights 2011/83/EU (article 6)
- ❖ Services in the internal market 2006/123/EC (article 22)
- ❖ General Data Protection Regulation (GDPR)

› The identity details view **by itself** does **not** trigger users to avoid giving personal data to no-identity websites. To do that, we must bring back the **user warning** against disclosing personal data to no-identity sites (see later slides)

Fourth, require standard identity view on data entry

09:25

Example B.V. Noord-Holland, NL

example.com/l

EXAMPLE .com

Please sign in

Email address

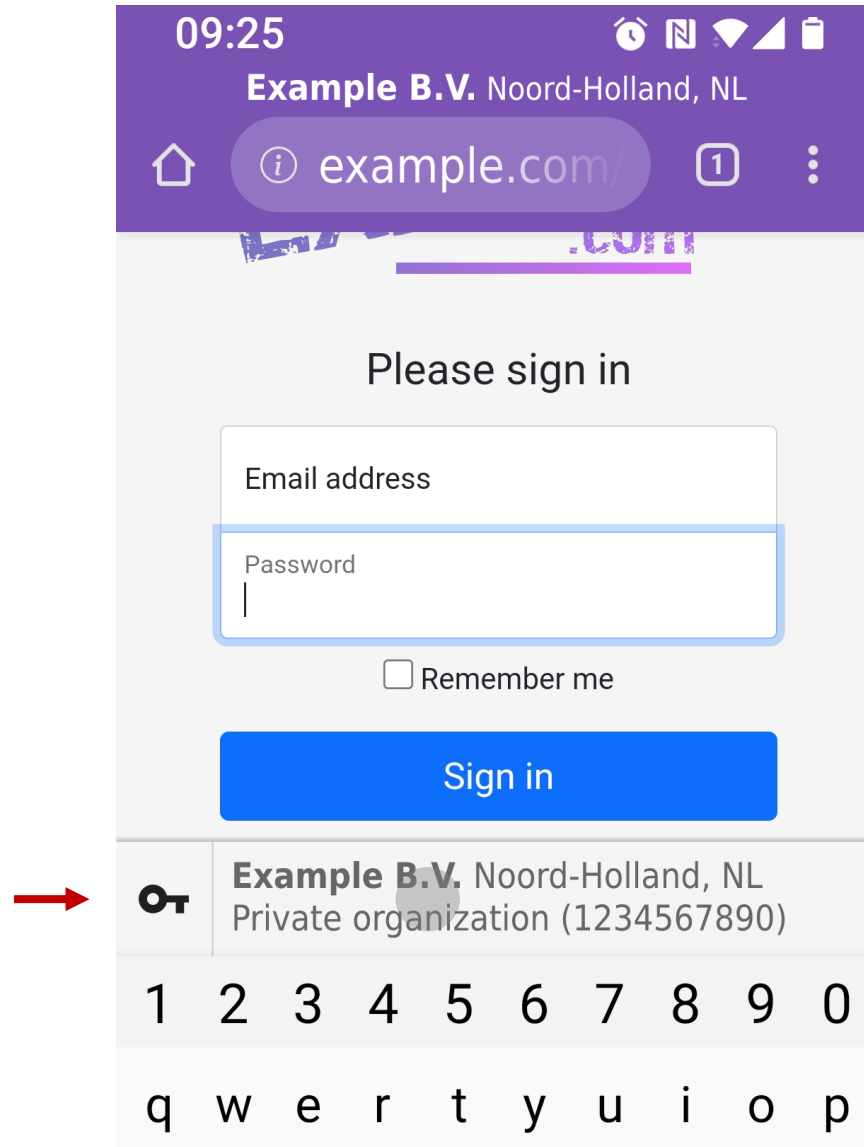
Password

Remember me

Sign in

- ▶ Watch what happens on QWAC/EV site when a user selects an input field before personal data is provided

Fourth, require **standard identity view** on data entry



- › Identity summary appears above the keyboard
- › This helps users identify website owners with a “high degree of certainty”
- › Click the identity summary to show detailed identity information

Fourth, require **standard identity view** on data entry

The screenshot shows a mobile browser interface. At the top, the status bar displays the time 09:25 and various icons. Below it, the browser title is 'Example B.V. Noord-Holland, NL' and the address bar shows 'example.com/'. The main content area has a heading 'Please sign in' and two input fields: 'Email address' and 'Password'. Below the password field is a 'Remember me' checkbox. At the bottom, there is a detailed identity view for 'Example B.V.' with a back arrow, an information icon, and a lock icon with a checkmark. The address is 'Nieuwezijds Voorburgwal 147, 1012 RJ Amsterdam, Noord-Holland, NL'. Below the address is 'Private organization (1234567890)'. A numeric keypad and a QWERTY keyboard are visible at the bottom of the screen.

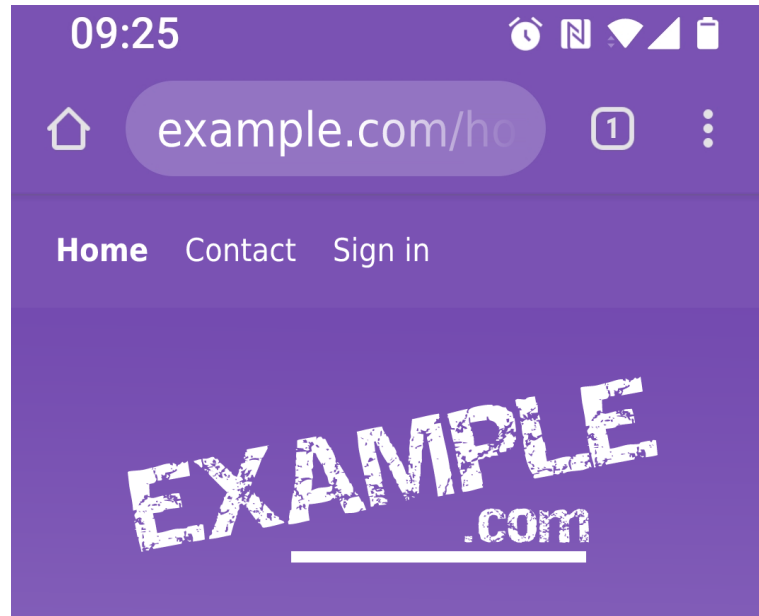
➤ Showing detailed identity

- An EU statement or symbol could be shown with the identity details. In future we could add other verified data elements (privacy policy, ISO 27701, phone numbers, social media)

Fourth, require **standard identity view** on data entry

- ▶ The **identity summary and identity detail helps users identify website owners with a “high degree of certainty”**
- ▶ This also encourages users to review the website identity **before** submitting personal data
- ▶ This satisfies the EU requirements listed above (GDPR, eIDAS 2), as users will be informed about the recipient of their personal data before they submit

Fifth, require standard **no-identity** warning



All posts Archive Videos Subscribe

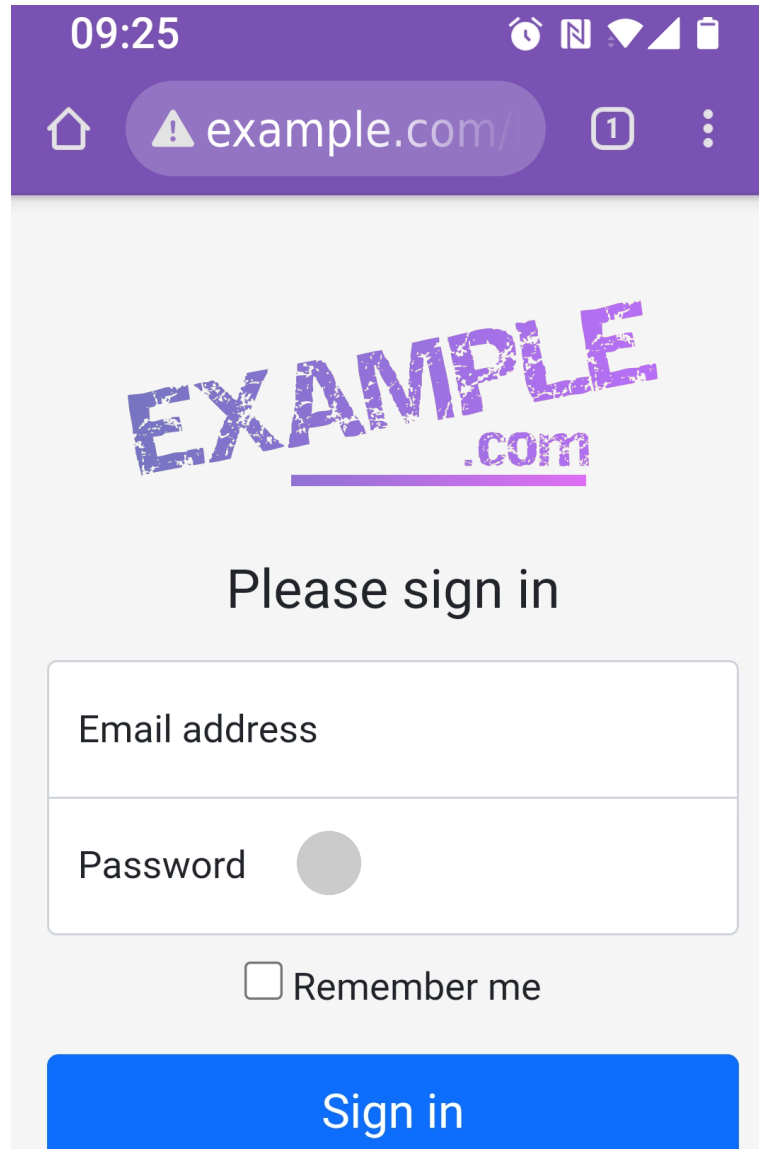
Welcome

by Chris Bailey - 22 September 2021

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Curabitur euismod ipsum quis libero feugiat scelerisque. Ut varius, leo nec rhoncus tincidunt, mi nisi rutrum dui, quis vehicula est turpis et nisl. Curabitur lacinia, leo sed vulputate volutpat, mauris justo laoreet nibh, rutrum viverra nulla risus vel magna. Praesent et facilisis dolor. Ut ac vehicula ipsum. Sed maximus arcu turpis, eu tincidunt neque elementum vel. Vestibulum eu

- › Websites with no identity have no symbol in the address bar
- › This UI assumes that the lock symbol will be removed for all encrypted connections.
- › No warning will appear so long as website does not ask for personal data

Fifth, require standard **no-identity** warning



09:25

example.com/

EXAMPLE
_com

Please sign in

Email address

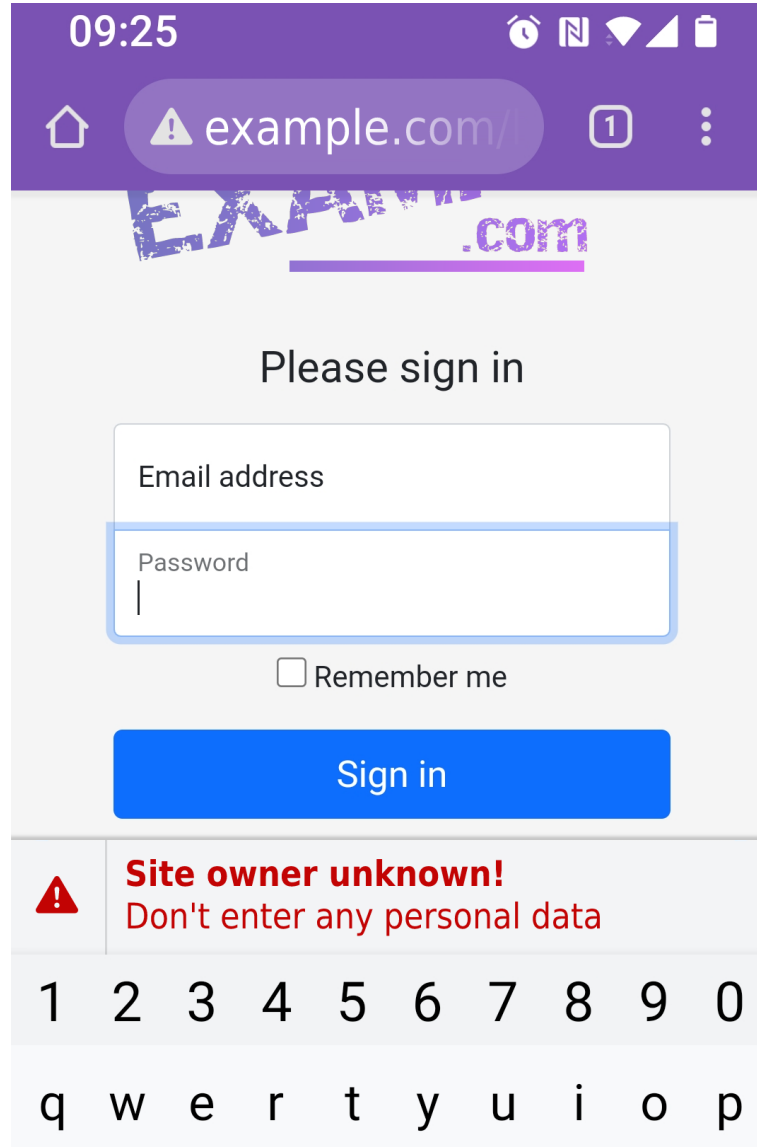
→ Password

Remember me

Sign in

- Include a warning symbol in URL if input field is on page
- Clearly warn users before they can type personal data

Fifth, require standard **no-identity** warning



09:25

example.com/

EXAMPLE.com

Please sign in

Email address

Password

Remember me

Sign in

Site owner unknown!
Don't enter any personal data

1 2 3 4 5 6 7 8 9 0

q w e r t y u i o p

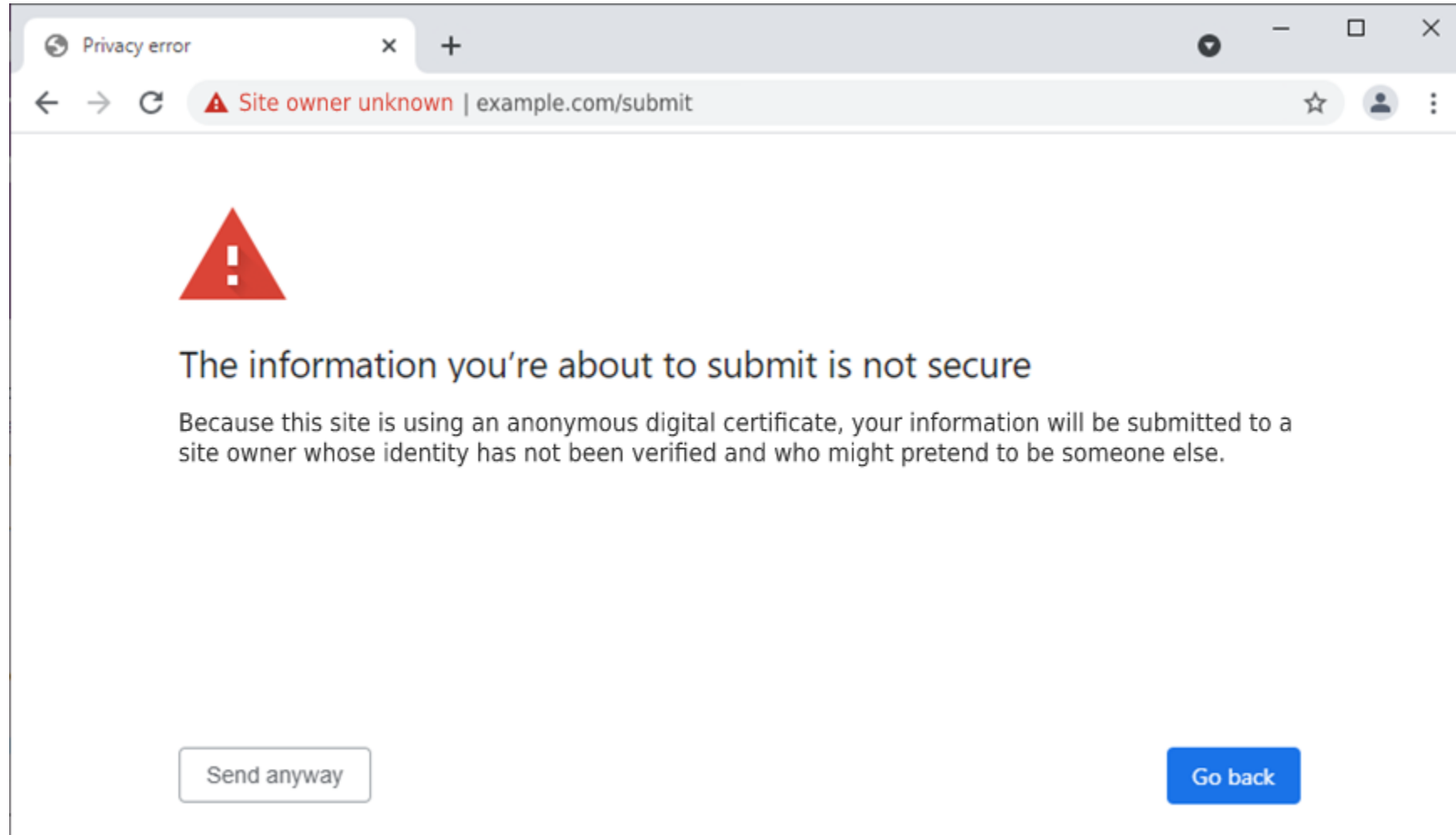
- This warning helps users reconsider when sending data
- Clicking the warning should provide the user more details about the risk, example in summary slides

Fifth, require standard **no-identity warning**

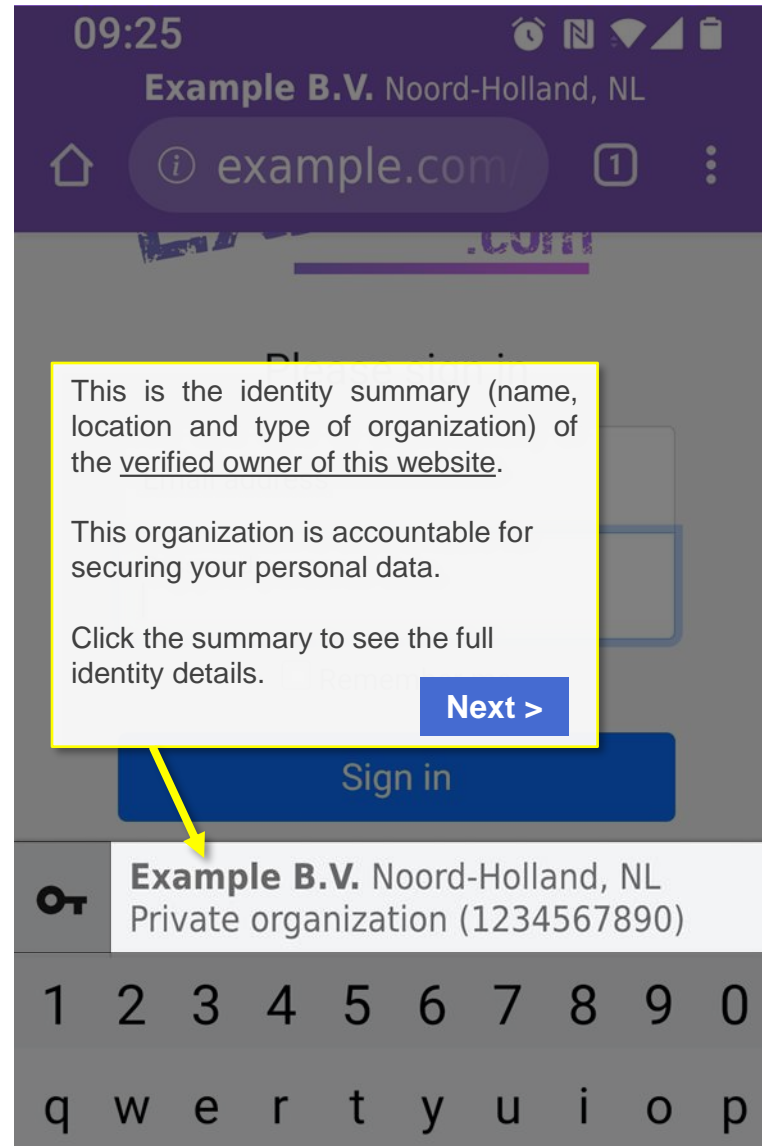
- The **warning on data entry** for anonymous sites is more effective in warning users
 - Minimal user education required
- But there are always users that ignore warnings
- Add interstitial (second warning) if user ignores first warning?

Require confirmation to send data to an anonymous site

Browsers have used this technique before



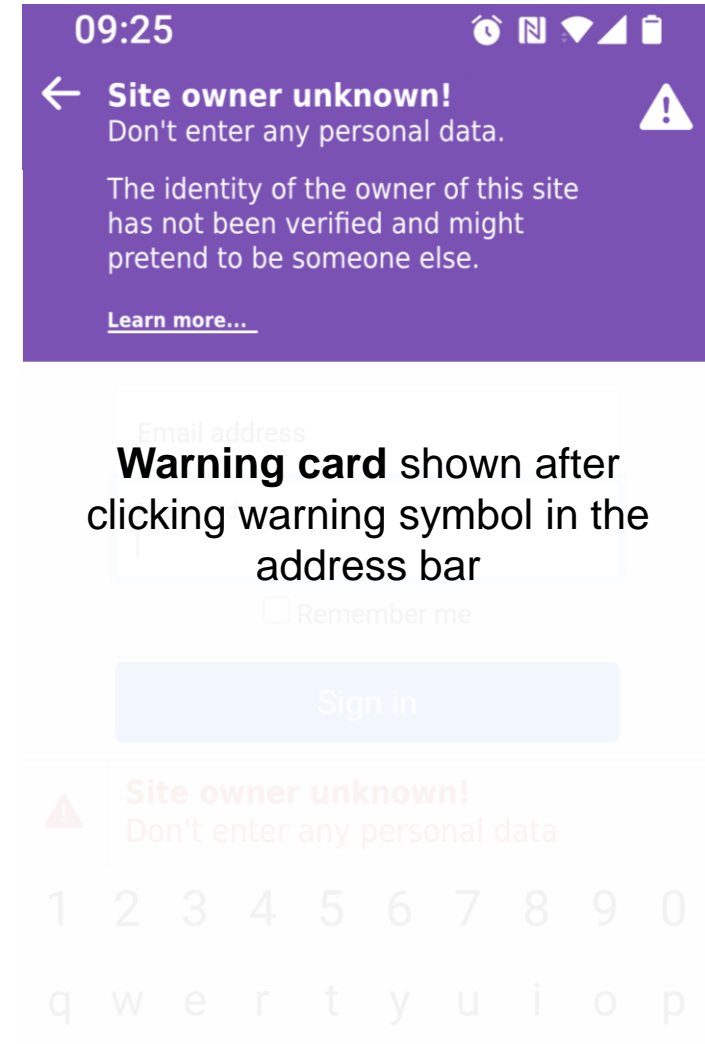
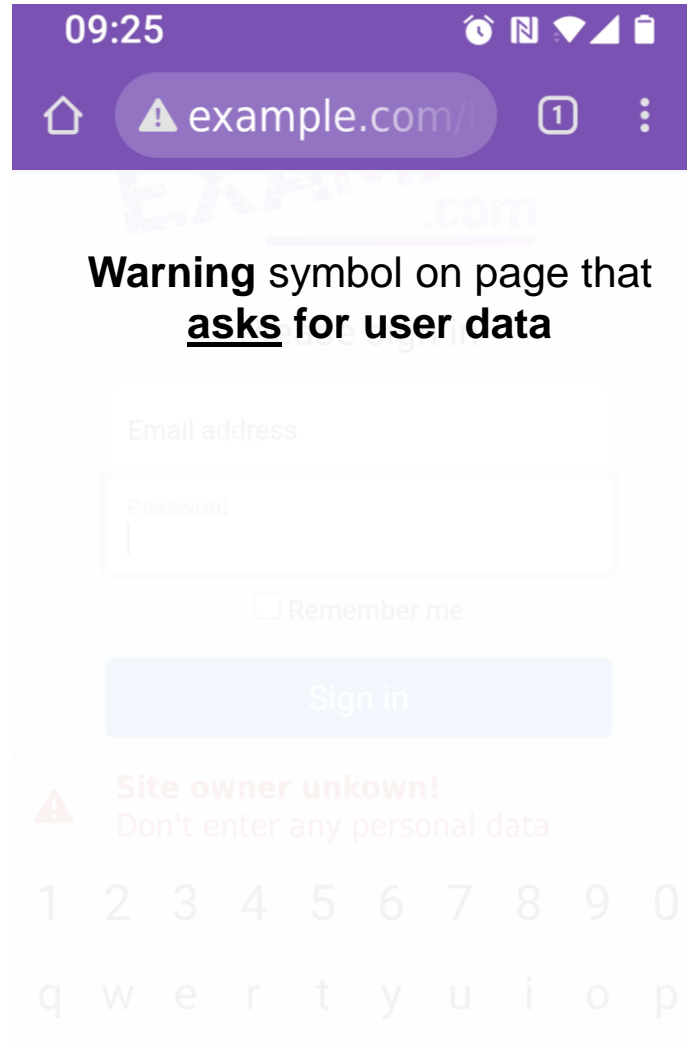
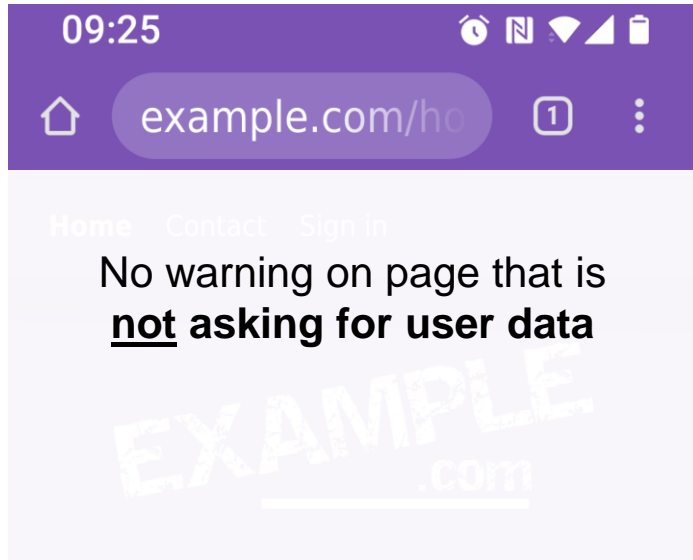
Education in browser via **interactive user guiding**



- **Interactive user guiding helps users to better understand security features**
- Content can be provided as text or in combination with animations and video
- Wizards can be shown
 - after a browser update
 - when a user encounters a warning or information for the first time
 - on user request
 - as reminder for high-risk sites

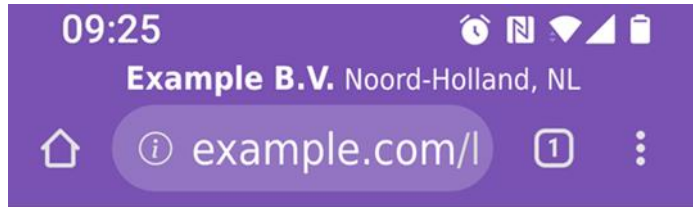
Summary of EU compliant header interfaces - no identity

DV - NO IDENTITY CERTIFICATE

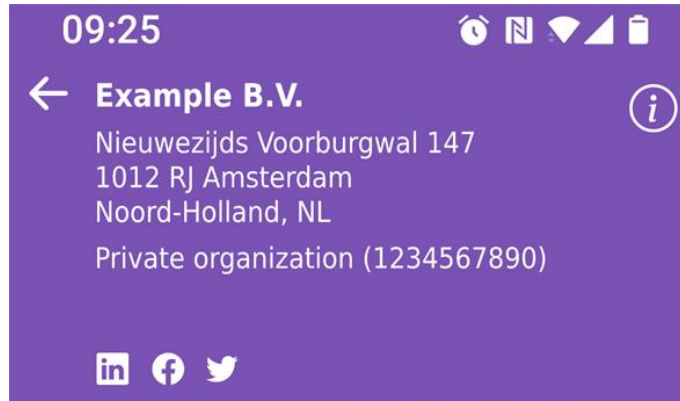


Summary of EU compliant header interfaces - with identity

QWAC / EV - IDENTITY CERTIFICATE



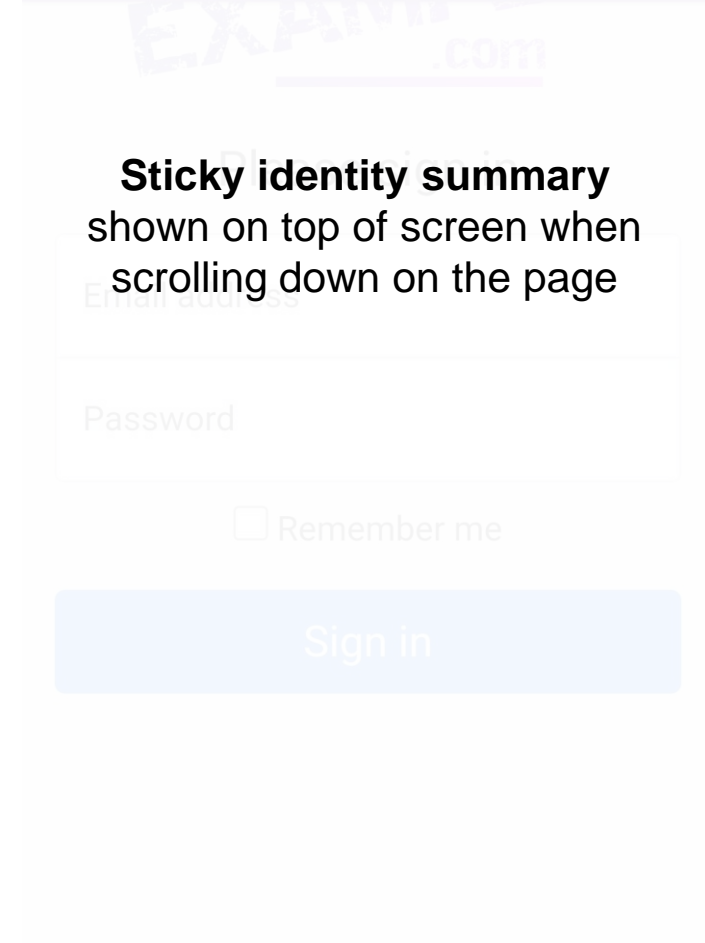
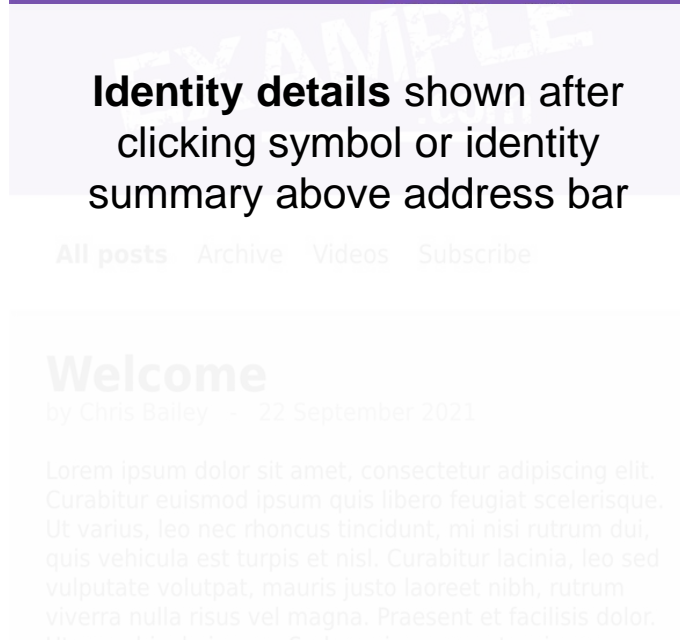
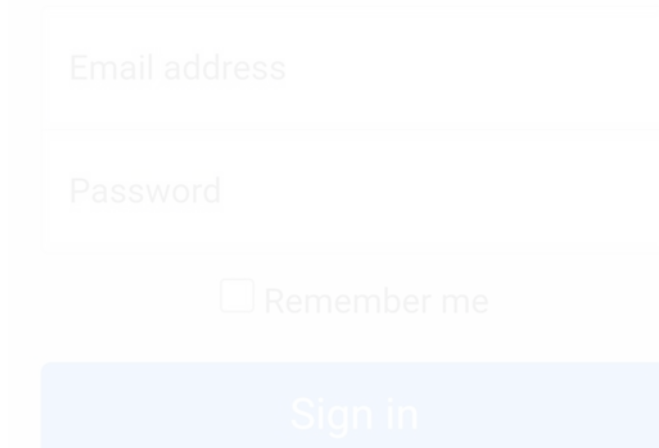
With or without asking for user data



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



Summary of EU compliant data entry interfaces

DV

09:25

Example B.V. Noord-Holland, NL

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

Please sign in

Email address

Password

Remember me

Sign in

Site owner unknown!
Don't enter any personal data

1 2 3 4 5 6 7 8 9 0

q w e r t y u i o p

QWAC / EV

09:25

Example B.V. Noord-Holland, NL

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

Please sign in

Email address

Password

Remember me

Sign in

Example B.V. Noord-Holland, NL
Private organization (1234567890)

1 2 3 4 5 6 7 8 9 0

q w e r t y u i o p

QWAC / EV

09:25

Example B.V. Noord-Holland, NL

Identity details above keyboard is shown because user clicked on summary

Please sign in

Email address

Password

Remember me

← **Example B.V.** (i)
Nieuwezijds Voorburgwal 147
1012 RJ Amsterdam
Noord-Holland, NL (lock)
Private organization (1234567890)

1 2 3 4 5 6 7 8 9 0

q w e r t y u i o p

Allow gradual phase-in



› Months 1-9

- Announce schedule for new UI and warnings
- Show pre-warnings in developer consoles

› Months 10-24

- Show the new Identity UI for site with an QWAC and EV certificate
- Show URL warning symbol for sites with data fields and DV certificates
- Show warning above keyboard if input field is selected for DV website
- Education in browser via interactive user guiding

› Month 25

- Require confirmation on submission for DV sites (slide 26)

This is similar to past successful browser schedules for http to https

Extend new identity UI to EV certificates

- QWACs are based on EV Guidelines
- There are ~128 EV certificates for every 1 QWAC in use
 - Many major websites already have EV
- Helps achieve eIDAS goals:
 - “Website authentication services provide users with assurance that there is a genuine and legitimate entity standing behind the website. Those services contribute to the building of trust and confidence in conducting business online, as users will have confidence in a website that has been authenticated.”
- Over time, harmonize QWAC and EV requirements

LET'S WORK TOGETHER TO MAKE THE
NEW eIDAS UI WORK!

THANK YOU!

QUESTIONS?

Chris Bailey

VP Trust Services

chris.bailey@entrust.com

+1.678.595.7999





ENTRUST

SECURING A WORLD IN MOTION