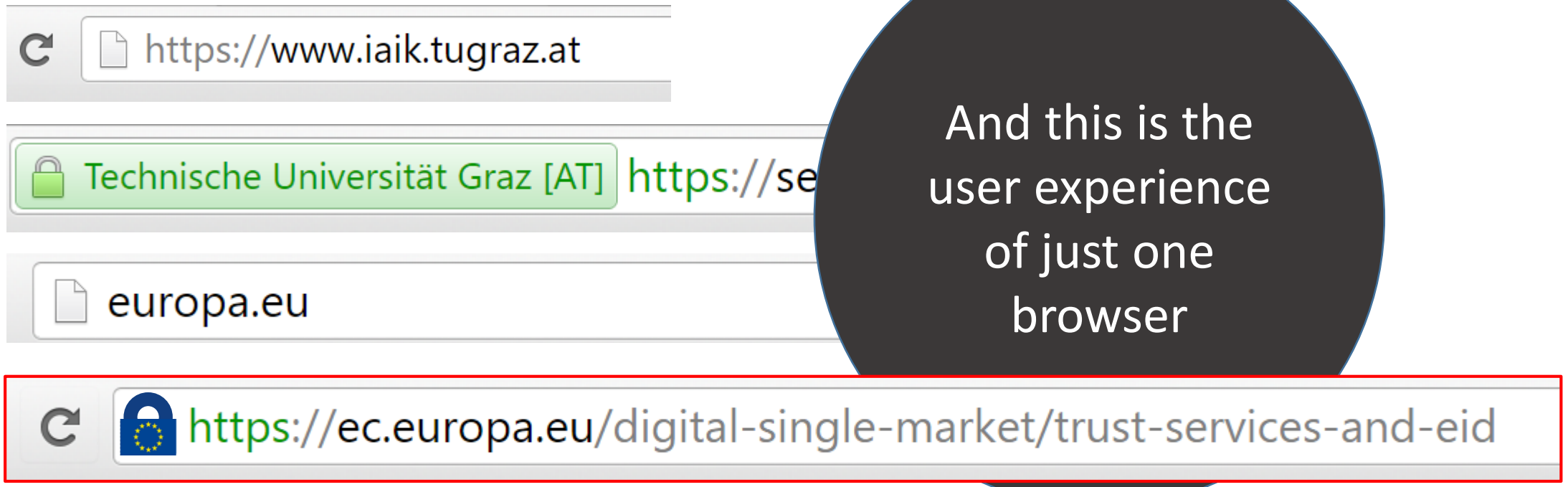
# WEBSITE AUTHENTICATION

# THE ISSUE TO RESOLVE

BROWSER LIABILITY

MEMBER STATE LIABILITY




And this is the user experience of just one browser

At this point in time websites are "stamped" with the URL-display as either "NO SECURITY (http)" or "SSL" (https) or with "SSL-EV" extended validation.  In all cases it is a validation where **browser provider** state the security level basing on external information. This needs a process where the CA is **approved by the browser provider.**

With eIDaS there is a **basic change** as concerns these assumptions. A further category is introduced where **approving is arranged by the Member States via the Trust-List**.

**This new situation is ineffective and close to useless unless browser providers reflect the situation properly by**

- Recognizing and technically supporting this new category
- Introducing a further "stamp" e.g. "Blue lock" to signal to the user.

(a)Unless validation bases on the Trust-List and - irrespective whether the CA is "approved" by the browser provider the browser provider will give false information to the user.
Liability when deployed in Europe might deserve discussion in such case.

(b)In case validation is performed by the browser for Trust-List based certificates this raises the question of the browser provider being a "trust service provider" or even a "qualified trust service provider" and the full range of supervision questions.

**We need a situation that can be handled by the browsers and returns all the trust the regulation asks for**

# A way to comply

- **We need a standardized (e.g. ETSI) encoding within a certificate that is managed via the trust list.**

- In case not all standardized encoding in a website certificate can be verified (e.g. "qualified website certificate“ ) the user will be notified just as he/she is notified today in case a certificate is not recognized by the browser.

- **browsers might provide a (standardized) interface (e.g. for a browser plugin provided by a qualified validation service) receiving the certificate with a non-fully verifiable encoding. Providing a verification result in a eIDAS compliant manner.**

Ideally this "plugin" could also pass the "stamp icon" (e.g. blue lock or other according to provider and result) to the browser.

# Result

- Governments and industry e.g. banking could effectively use such services according to eIDAS with the expected benefit. This would result in a substantially increased technical and legal certainty.
- The source of the information and the quality (resulting in a jurisdiction aware communication) can be grasped and demonstrated to the user.
- The method can accommodate if others (US etc.) also introduce trust that is backed up by the legal system