THIS IS NOT MANDATORY, YOU WILL NOT NEED TO HAVE AN EUID. WHAT IS MANDATORY IS FOR ALL EU MEMBER STATES TO HAVE AN OPTION TO GIVE CITIZENS AN EUID IF THEY REQUEST ONE.

- DATA is not stored centrally. Instead you will have a Wallet application running on your device(your digital ID/PID will be securely tied to your specific wallet on your device to prevent identity theft **[1]**) that will store your cryptographically signed digital documents that will be issued to you by TRUSTED ISSUERS(e.g Governments, Universities etc.). All data will be stored **LOCALLY** on this wallet. **THERE IS NO CENTRAL DATABASE WHERE YOUR DOCUMENTS AND INFORMATION ARE BEING STORED FOR THIS PURPOSE.**

- **Qualified Electronic Attestations of Attributes (QEAA)** which are Issued exclusively by or on behalf of **Qualified Trust Service Providers (QTSPs)** and **Public Electronic Attestations of Attributes (PuB-EAA)** which are Issued by or on behalf of **public sector bodies** or official authorities when the data originates from official registries or government databases. Issuers of QEAA and PuB-E are required to provide **PRIVACY ORIENTATED** methods for verifying that the information being provided to the **Relying Party(e.g the website)** is valid. **[2]** expand on this at the bottom please check.

- This will allow the user of this wallet to **SELECTIVELY PROVIDE ONLY THE REQUESTED INFORMATION**. Assume, that a website is requesting to see if you are above 18, so instead of providing your whole legal document, or even your DOB or exact age, you can just provide them a YES/NO(Basically, Yes I am above 18 or No I am not above 18) - note that this will be accompanied by information that will allow the Relying Party to validate your **Wallet Unit(**Basically whether you are using a **TRUSTED WALLET SOFTWARE** and **If the wallet unit is actually connected to your PID) + EAA** and/or **PID**. Personally this is such a good and private way to verifying information without needing to actually provide documents or anything to every random website.

- MANY THE TECHNICAL PARTS MEANT TO BE USED BY THE WALLET CLIENT, THE ISSUER etc. are OPEN SOURCE. THAT MEANS THERE IS GOING TO BE A LOT OF SCRUTINY OVER WHAT'S ACTUALLY GOING BEHIND THE SCENES. WHICH IS EXTREMELY GOOD FOR SECURITY AND PRIVACY.

---

[1] - The PID is a set of core personal attributes (e.g your name, surname, date of birth, nationality etc.) that uniquely identifies you. It serves as the most fundamental proof of your identity in the digital realm, providing a high level of trust and assurance for various online and offline services. It is securely stored in your EUDI Wallet on your personal device and is cryptographically bound to your specific wallet unit. They are issued by **trusted public authorities**, typically **national governments** or designated public sector bodies within each EU Member State.

[2] - **Qualified Trust Service Providers (QTSPs)** and **PuB-EAA** Providers will provide ways to verify that the data you are providing is valid. So let's use something like "Are you above 18?" as an example. So, you provide them the answer "Yes" to the previous question. After the **Relying Party** gets that answer, they have to first verify that you are using a valid Wallet Unit, and then check that the information you provided is actually valid or not. In this case since this is an 'above 18' inquiry, they don't necessarily receive or validate your full DOB. Instead, they check the validity of your PID (which *contains* your DOB) to trust the specific 'age_over_18' attribute provided by your wallet. So, your government will provide methods for the Relying Party to check if your *PID* (and therefore its derived 'age_over_18' attribute) is valid/invalid/revoked. If this was another **EAA** (e.g., your degree), the Relying Party would first validate your Wallet Unit. Depending on the service's requirements, they may also authenticate your PID, and then they will definitely use the verification method provided by the EAA issuer to confirm the EAA's validity and non-revocation.

Now since this makes the **Relying Party** ask another entity(a verification method provided by your government and EAA provider), there is a chance that this entity can track your internet usage(like assume your university sees that huh, these websites have asked to verify the credentials of this student, that means this student has been visiting websites). BUT there is a very strong statement that **QUALIFIED ISSUERS*** must maintain **Unlinkability of Transactions** aka make it super duper near impossible to track you. There are quite a few ways this can be done, But the **methods for achieving this unlinkability are guided by the EUDI Wallet's common specifications and regulations**, which aim for standardized, privacy-preserving approaches to revocation and transaction handling, not entirely left to issuer discretion

* So note that I stated **QUALIFIED** before Issuer. That means there are Unqualified Issuers. So there's going to be a list of Issuers who have been vetted extensively to make sure that they are following all requirements and then they'll put on a list basically saying that these ones are trusted. But that means, that Unqualified Issuers are not held to the same standard,. Like, an example of an unqualified issuer might your Gym, and they can give you an EAA for your gym card, but they might not be following many of the legal requirements that a Qualified Issuer should be. But they should still be at the very least following the technical requirements specified in the common specifications.