ONE DIGITAL EDUCATIONAL IDENTITY FOR VOCATIONAL EDUCATION, HIGHER PROFESSIONAL EDUCATION, AND UNIVERSITY EDUCATION

Vocational education, higher professional education, and university education are working toward a single shared digital education identity. This will facilitate student mobility between institutions, give learners more control over their own data, and reduce error-prone manual administrative work at educational institutions.

In this paper, we explain how SURF views and is working on a digital identity for higher education. The first part discusses why a single digital education identity is important and what we mean by it. In the second part, we discuss important building blocks. The third part deals with implementation in the Netherlands and coordination with European developments.

1. VISION FOR DIGITAL EDUCATIONAL IDENTITY

First, we explain why a single digital educational identity is important for further education. We also explain what we actually mean by a single digital educational identity and what the key considerations are.

Towards a single digital educational identity for vocational education, higher professional education, and university education

The issues in society and on the labor market, and the changing needs of learners, call for flexible education and learning without barriers. That is why vocational education, higher professional education, and university education are working to shape an education sector that is experienced by learners as a single coherent educational space, in which all learners are in control of their own learning pathway without administrative barriers – both for the original student and the lifelong learner. This enables educational institutions to offer every learner the most appropriate education. To make this logistically and administratively feasible, it makes sense for learners to have a single, institution-independent digital identity that they can use at any educational institution. An identity that stays with

you throughout all stages of your education, even if you change educational institutions, and remains with you after you have completed your studies. This is in contrast to the current situation, where individuals have a separate identity at each institution where they follow a program, subject, or course, including a significant amount of paperwork to transfer study results achieved at one institution to the administration of another. Furthermore, these identities disappear as soon as the education is completed.

The advantages of a single digital education identity are:

- it puts the learner at the center of education: you move as a person through education and through systems, not the other way around;
- it facilitates learner mobility between courses, institutions, and sectors;
- it supports lifelong learning, because the educational identity can continue to exist after the original program, and learners can continue to link proof of their results to it;
- it facilitates the development of a single, easily accessible educational space in the Netherlands, Europe, and beyond.

Keeping control of identity-related facilities

When working towards a single educational identity, it is not only important that learners have control over their data. It is also essential that the education sector has and retains control over the digital landscape surrounding identity. Identity plays a key role in providing access to and using crucial digital education systems, such as digital learning environments and student administration. If educational institutions leave this entirely to market parties for the sake of convenience, efficiency, and ease of use, there is a risk that education will become dependent on suppliers and that there will be no easy way out. Important public values for education, such as privacy, freedom of choice, transparency, and digital independence, may then lose out to commercial interests.

Digital educational identity and the facilities surrounding it are so important for the digital sovereignty of education that the education sector must organize this itself in order to safeguard public values. If vocational education, higher professional education, and university education do this jointly, individual institutions will trade some leeway in choosing their own digital solutions, but they will gain autonomy in return as a joint education sector.

Citizen service number and DigiD for education?

For civil affairs, residents of the Netherlands already have a single digital identity, namely the combination of their citizen service number (BSN) and DigiD. Is it possible to use this for digital educational identity? No, the BSN and DigiD cannot be used for this purpose. Nor is this necessary: people have identities in different contexts, both as individuals and in digital systems. As a citizen, different characteristics are relevant than as a student or patient. It is quite conceivable that a lifelong digital educational identity will be part of a number of core digital identities in the future, alongside those for government, work, financial affairs, healthcare, and social activities, for example. For the sake of user privacy, but also for operational reasons, it is wise not to link all these identities in digital systems.

DigiD and education

DigID works with the citizen service number (BSN), a unique personal number that every Dutch citizen receives when registering in the Personal Records Database. The use of the BSN is well protected.

DigiD is not suitable for use in education. There are several reasons for this:

- The use of DigiD is only permitted in processes that are specifically mentioned in a law. For example, the education sector may use DigiD when registering for a course. DigID is not permitted for other processes, such as gaining access to and logging in daily to specific applications.
- The national government is in charge of DigiD; the end user has no influence on what data is linked to it.
- Working with DigiD would mean that applications receive the sensitive citizen service number and can immediately recognize a person by it. This carries the risk that a very personal profile of someone can be built up without their knowledge.

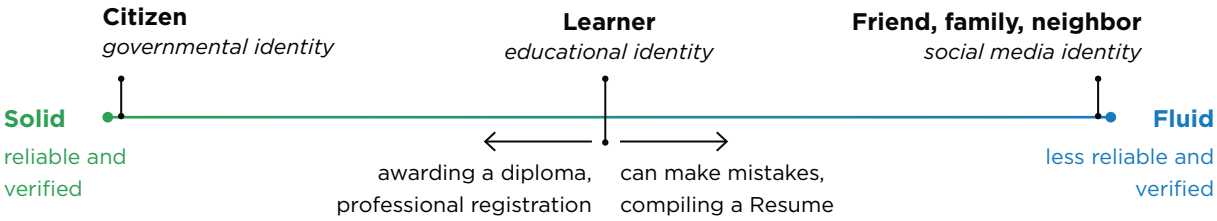

Figure 1: reliability of different identity types

Identity is a unique sum of characteristics

Identity is who you are – as a person and as a digital user. In social life, identity is the sum of characteristics that make you unique: think of your name, where you come from, and what you do. Your identity is expressed in various contexts, such as friend, learner, colleague, or parent. These contexts differ and can change, but they all belong to you.

In digital systems, identity is mainly about recognition: being able to prove who you are, what characteristics belong to you, what you can do, and what you are allowed to do. In education, for example, you are a student, you have achieved study results, you have access to a digital learning environment, and you are allowed to use an institution's subscriptions and applications.

In short: your identity is not only who you are in the real world, but also how you are recognized and represented in digital systems. Both go hand in hand.

More control for the learner

A single educational identity plus the option to decide whether or not to share their data gives learners more control. By control, we mean that learners have insight into what happens to their data and that they have influence and choices where possible. Complete freedom of choice is not possible in the context of education; certain data is necessary for the provision of education. For example, a teacher must be able to monitor a learner's study progress, and an educational institution needs confirmed study results in order to award a diploma.

Identity in social existence	Identity in the digital world of education
Who you are – a unique human being	Characteristics traceable to one specific person
What belongs to you	Characteristics that belong to you as a person, such as your address, but also dyslexia, for example
What you can do	Verifiable competencies and qualifications, such as diplomas and micro-credentials
What you are allowed to do	Capabilities that belong to your role within the educational institution (such as learner, teacher, researcher, etc.), authorizations that have been assigned to you

Figure 2: social identity versus identity in the digital world of education

Self Sovereign Identity

Self sovereign identity (SSI) is a concept that often comes up in the context of identity and self-determination, as an alternative to how identity is currently usually regulated. In essence, SSI is a digital identity that users create and manage themselves, with complete control over their own identity data. In education, SSI in its purest form is not applicable, because complete control over one's own data is not possible for a learner.

Control for the learner ties in well with the fact that an educational identity has *solid* and *fluid* elements. By solid, we mean that, for example, the awarding of a diploma or professional registration must be a very reliable process. The person who receives a diploma must also be the person who actually earned it. Fluid means that learners must sometimes be able to choose for themselves what information they want to share about themselves. For example, does a teacher in a follow-up course need to know what grade you received for your first internship? Education is about learning, and people—especially young people—must have the space to develop, change, and choose how they want to present themselves.

In summary

A single digital educational identity for higher education promotes student mobility and lifelong learning. It puts the learner at the center of education, rather than digital systems. If learners can choose whether or not to share data, it gives them more control over their identity—just as people have in everyday life. By keeping control of the digital landscape surrounding educational identity, the education sector strengthens its digital sovereignty.

2. IMPORTANT BUILDING BLOCKS

A number of building blocks are needed to achieve a single digital educational identity. The most important ones we discuss here are eduID and the wallet. Organizational agreements and trust play a crucial role in both, which is why we also briefly discuss the importance of trust networks.

eduID: foundation for a Dutch digital educational identity for vocation, higher professional, and university education

eduID forms the foundation of a single digital education identity for Dutch secondary education. It is a personal, unambiguous basic identity that can be used anywhere in vocational education (MBO), higher professional education (HBO), and university education (WO) to prove who you are. eduID uses a minimal set of data to work properly for various applications, specifically: first name, last name, email address, role at the institution(s), and multiple identifiers. eduID does not store any other data. No more data is processed than is strictly necessary, privacy is guaranteed, and data remains at the source as much as possible.

eduID is ready for use and is about to be implemented on a large scale in higher education. In time, learners will be able to create a new eduID or link an existing eduID when enrolling for a course. Vocational education, higher professional education, and university education have committed to implementing eduID in 90% of institutions by 2031.

Identifier
An *identifier* is information used to recognize a person digitally, such as a number. eduID uses specific identifiers for specific services. Because eduID uses a separate identifier for each service, information from different systems can only be linked with the user's approval.

Figure 3: role of learner wallets towards issuers and verifiers

A digital wallet for exchanging data

A so called 'wallet' provides the option to storing and exchanging data about yourself. From 2027, EU member states must offer citizens a wallet based on agreed standards and with a similar user experience. Wallets offer interesting opportunities for education. There are promising applications for access to education and digital systems (via eduID, among others) and for exchanging study results, whereby the learner retains control over their own data with the wallet. Important to emphasize: eduID can be stored in a wallet – just like your ID card in your wallet – so a wallet is not a replacement for eduID.

How does it work? With a wallet, a learner can collect verifiable data from an *issuer*. This could be an educational institution where a study result has been achieved. If another education institution (the verifier or verifying party) needs confirmation of that study result for admission or exemption, the learner can share the study result. Because the study result is digitally signed by the issuer, the data is reliable (*verified*).

Advantages of working with a wallet include:

- The learner is positioned between the issuer and the verifier; this 'separation' allows the learner to better protect their privacy.
- Learners only need to share what is necessary. Measures are being developed to protect users from sharing more data than is necessary.
- Thanks to an underlying trust network of issuers and verifiers, verification of data can be automated, eliminating the need for manual work.

Our vision of (digital) identity and the most important technical building blocks are summarized in the figure below. On the left is the human side of identity, on the right is its representation in digital systems.

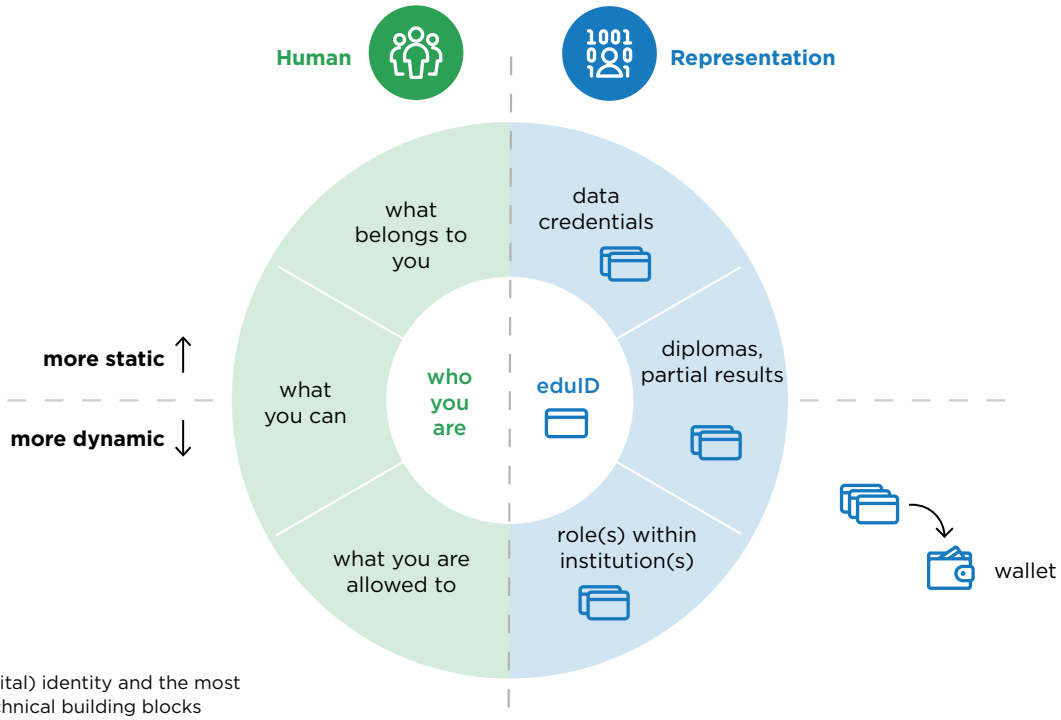

Figure 4: (digital) identity and the most important technical building blocks

A trust network is crucial

Applications such as wallets require a trust network or *trust framework*: issuers and verifiers must trust each other. Working with a single educational identity contributes to mutual trust between participants in a trust network. Federative solutions fit in well here: in a federation, members collectively build and maintain agreements about trust, protocols, and interoperability. In educational federations, some things are regulated centrally by one of the participants (such as eduID by SURF) and other things are left decentralized (for example, granting authorizations to users by educational institutions).

SURFconext is an example of such a federative solution. SURFconext allows users to log in to all cloud services used by an educational institution with a single username and password. With more than 190 affiliated institutions (more than 2 million users) and nearly 3,000 affiliated cloud services, SURFconext is a successful example of a large and well-functioning trust network.

In summary

eduID is a personal, unique basic identity for learners to prove who they are anywhere in secondary vocational education, higher professional education, and university education. It forms the foundation of a single digital educational identity. eduID is being widely implemented in Dutch secondary education. A wallet is a digital wallet for storing and exchanging data about yourself. Wallet users only need to share what is strictly necessary, allowing them to better protect their privacy. Thanks to an underlying trust network, shared data can be checked automatically, eliminating the need for manual work. In the near future, wallets will offer interesting opportunities for education, including organizing access to education and digital systems, and exchanging study results.

3. IMPLEMENTATION AND COOPERATION

The transition to a single digital educational identity for learners in vocational education, higher professional education, and university education will not happen overnight. In this final section, we briefly discuss implementation in education, European cooperation, and guiding principles for the future.

Broad implementation within educational institutions is needed

eduID is organized for and by the education sector, without commercial interests and with an eye for public values such as privacy. Educational institutions can benefit greatly from a single digital education identity that puts the learner at the center. It is a prerequisite for flexible education that enables learning without barriers for the learner. It contributes to the simplification of administrative processes and systems and reduces error-prone manual work.

The sector can only realize the full potential of eduID if everyone uses it. That is why broad implementation in secondary vocational education, higher professional education, and university education is necessary. This requires time, human resources, and constructive collaboration. Institutions have shown in the past that they can do this, for example with SURFconext, but also with the joint organization of enrollment and registration.

In Npuls, vocational education, higher professional education, and university education are working together with SURF to further develop the new way of working with eduID and wallets. This is not only a technical change, but also an organizational one. In addition, attention needs to be paid to learning how to make use the new possibilities: for learners, teachers, institutions, internship companies, and other stakeholders. The change will be implemented in stages. In the first phase, the existing institutional identities and eduID will continue to coexist.

Coordination across national borders

Student mobility does not stop at national borders. For a successful Dutch digital education identity in vocational education, higher professional education, and university education, it is therefore important to keep up with developments in Europe and beyond. In Europe, countries deal with education identity in different ways; solutions that are successful in the Netherlands are not always applicable in other countries – and vice versa. For example, the Netherlands is not allowed to use DigiD widely for education, whereas other countries can use something similar.

A number of European countries are also working on an eduID variant; it has the same name, but often a different conceptual and/or technical interpretation. Developers from different countries are seeking each other out and trying to streamline and align the different variants. In this way, they are building interoperability from the bottom up. This way of working together has proven to be more promising than imposing central solutions from the top down. This is because it allows much better consideration to be given to the specific circumstances in the different countries. Eduroam—the global, secure Wi-Fi network for education and research—was created in this way, for example.

Guiding principles

There is still much to be done in the Netherlands and internationally. When developing Dutch solutions and coordinating with other countries and European initiatives, SURF applies the following principles as guidelines.

- Solutions are user-friendly, offer added value for the user, and fit in with the 'journey' that learners take in education.
- Security and privacy are guaranteed as a matter of course.
- Digital systems are reliable and robust.
- Interoperability – the seamless collaboration of digital systems – is regulated on the basis of open standards and with transparent decision-making and management.
- The education sector strengthens its digital autonomy, and we prevent vendor lock-ins.

In summary

To reap the full benefits of eduID, broad implementation in secondary vocational education, higher professional education, and university education is necessary. This requires time, human resources, and constructive collaboration. We are working step by step: for the time being, the existing institutional identities and eduID will continue to coexist. Because student mobility does not stop at national borders, coordination with other European countries is necessary. The context of each country differs, which is why SURF believes most strongly in an approach in which countries work bottom-up towards interoperability between their digital solutions. SURF's compass is focused on user-friendliness, security, privacy, reliability, good governance, and maintaining the autonomy of the education sector.

READ MORE

www.surf.nl/en/themes/identity-access-management

CONTACTPERSON

Michiel Schok: michiel.schok@surf.nl