Driving innovation together

# HOSA: ARCHITECTURE FRAMEWORK FOR DIGITAL SECTOR SERVICES OF THE FUTURE

## Domain architecture for Identity & Access

| | |
|---|---|
| Authors: | Peter Leijnse, Domain Architect HOSA IAM<br>Menno Scheers, Lead Architect HOSA |

| | |
|---|---|
| Version: | 1.0 (English) |
| Date: | 21 March 2023 |
| Driven by: | CIOs of the higher education institutions, Higher Education Architectural Council, SURF, and so on. |

This publication is licensed under a Creative
Commons 'Attribution 4.0 Unported' licence.

## Foreword

We are pleased to present the HOSA Domain Architecture for Identity and Access. It is the end result of a two-year long collaborative process between architects, information managers and specialists, from institutions and sector partners.

The domain architecture outlined here shows what the landscape for identity and access in education and research should look like in three to ten years' time. The ambitions of the higher education sector, changes in research and education and international developments, including in relation to technology, have been taken as the starting point. The domain architecture is similar to a zoning plan and includes a vision of the future of the domain and the associated processes and systems. This vision also forms the basis for a roadmap to realise and set priorities for the domain architecture. This document therefore provides a framework for elaborating and assessing subsequent architectures and designs.

The other HOSA domain architectures, for Flexible Education and Research Data Management, employ the concept of business platforms to address the pressing need to facilitate collaboration of all types. The Identity and Access domain architecture serves to support this and outlines how the identification, authentication and authorisation of users, providers and services can be managed consistently across different business platforms. This is because these aspects are present in multiple platforms in a flexible architecture. The emphasis in doing so has been firmly on public values.

With the shift from centralised and federated provider-centric solutions to decentralised user-centric solutions, the IAM domain is undergoing significant change. A number of concepts described in the domain architecture have already become part of the conversation within and beyond higher education institutions, such as in the vocational education and training sector. It is also apparent that several 'future' developments we describe, such as credentials and wallets, have been moving at pace in recent times. In the domain architecture, we outline how current generations of IAM systems can grow into a future-proof architecture.

The Enterprise Architecture team at SURF will maintain and continue to develop the domain architecture in tandem with the sector.

# Contents

# 1 Introduction

## 1.1 Motivation

Higher education institutions are anticipating that the number of cross-institutional initiatives will grow and this will have a greater impact on their own services. The Dutch Acceleration Agenda for educational innovation in collaboration with ICT drafted by the higher education sector and various sector partners is such an initiative. UNL (the Dutch universities association) is also investigating the areas universities want to invest in together, such as research facilities, ICT for educational reform, and sustainable operations management. Higher professional education is also collaborating across institutions, for example on the subject of research support. The CIOs of institutions, SURF and a number of sector partners have therefore taken the initiative to create a joint architecture for the digital sector services of the future.

The developments in the area of more flexible education, lifelong learning (LLO) and data management are leading to more cross-institutional collaboration and organisation for common information and ICT services (sector services). Questions that arise in this regard include: “How do we ensure sector services are future-proof?”, “How do we ensure consistency in sector services?”, “How do we make reuse possible?”, and more recently, “How do we assure, protect and promote public values in the digitalisation of education and research?”.

Sector partners such as SURF, Studielink, DUO, DANS and NWO are trying to facilitate and support all institutions in this as much as possible. However, this is a complex process that creates a need for a joint architecture: for the sector-wide definition, development and deployment of information and ICT services, it is necessary to provide clarity about the demand for these services, the associated requirements in this regard, the design and configuration of these services, and services provided to institutions by ICT service providers. We want to create this common framework based on an architectural approach: the Higher Education Sector Architecture (Hoger Onderwijs Sector Architectuur or HOSA).

## 1.2 Goals

The HOSA project aims to define an architecture for sector services that are important for strategic collaboration between higher education institutions, sector partners and market players. HOSA is therefore based on the optimal articulation of the sector's demand with regard to sector services, defined in an objectives structure (see 2.4). It provides a facilitating framework for interoperability between institutions and providers of common ICT services. HOSA must play its part in ensuring that current and new sector service initiatives are established more quickly and in a more future-oriented and future-proof way. Sector partners and market players in ICT services can effectively respond to this with their service portfolio.

## 1.3 Scope of the domain architecture

In principle, the scope of the domain architecture is the Dutch higher education sector (higher academic education and higher professional education). The international context is also taken into account. The time horizon is the medium and long term (3 to 10 years), with an assessment of the functional needs for sector services for the education and research objectives. The architecture to support education and research has a broad sweep, focusing on services, processes, functionality, data and technology, governance, ownership, management and support. This is a conceptual description with guiding frameworks for solutions.

This domain architecture is a conceptual description of the intended setup of sector services with respect to identities and access. Identity and Access (also referred to as Identity & Access Management (IAM) is understood to mean enabling the correct 'identity' to 'access' the right facilities for the right reasons, under the right conditions and at the right time. Identity and Access needs to establish three important conditions for the delivery of digital services:

- Identification: that we know who you are and which digital identity belongs to you;
- Authentication: that we have a level of assurance that you are really the person to whom this digital identity belongs;
- Authorisation: that we know what actions you are permitted to undertake (whether or not authorised by someone else), and those you are not permitted to undertake.

This domain architecture for Identity and Access for education and research has a broad sweep and focuses on services, service delivery, processes, functionality, data and technology, privacy, information security, management, ownership, administration and support. This is a conceptual description providing guidelines and a framework for solutions.

## 1.4 The objectives structure

The goals of the sector have been summarised in the form of an objectives structure[1] that provides insight into the objectives and ambitions set by the sector. The foundation for this objectives structure is based on the strategic agenda of the Ministry of Education, Culture and Science. This has been supplemented by goals from other policy documents and included in the diagram below.

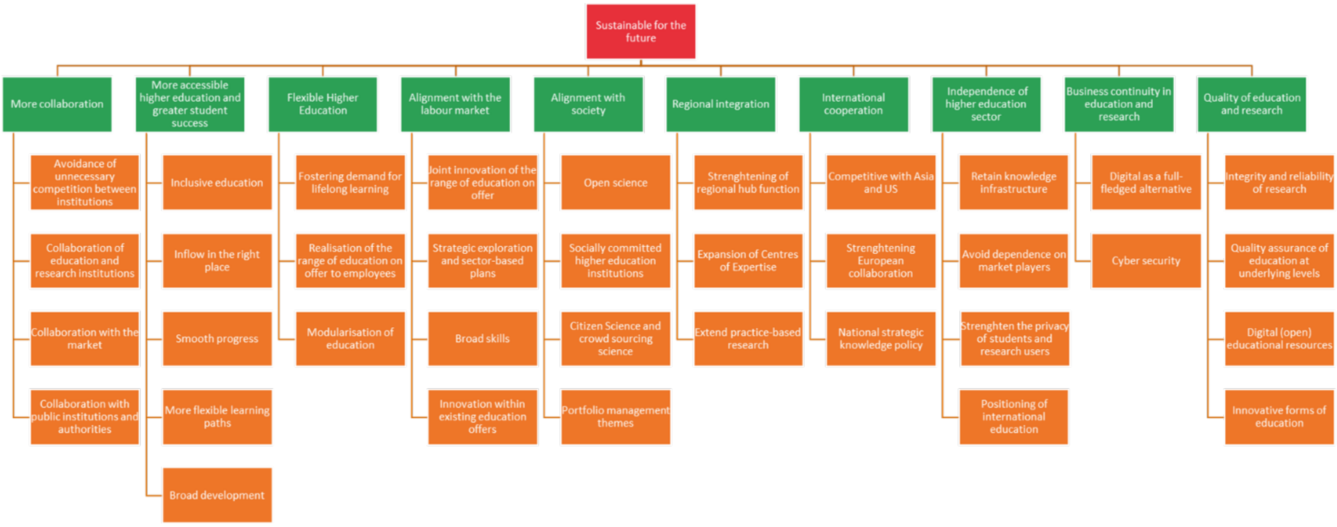

Sustainable for the future
More collaboration
Avoidance of unnecessary competition between institutions
Collaboration of education and research institutions
Collaboration with the market
Collaboration with public institutions and authorities
More accessible higher education and greater student success
Inclusive education
Inflow in the right place
Smooth progress
More flexible learning paths
Broad development
Flexible Higher Education
Fostering demand for lifelong learning
Realisation of the range of education on offer to employees
Modularisation of education
Alignment with the labour market
Joint innovation of the range of education on offer
Strategic exploration and sector-based plans
Broad skills
Innovation within existing education offers
Alignment with society
Open science
Socially committed higher education institutions
Citizen Science and crowd sourcing science
Portfolio management themes
Regional integration
Strenghtening of regional hub function
Expansion of Centres of Expertise
Extend practice-based research
International cooperation
Competitive with Asia and US
Strenghtening European collaboration
National strategic knowledge policy
Independence of higher education sector
Retain knowledge infrastructure
Avoid dependence on market players
Strenghten the privacy of students and research users
Positioning of international education
Business continuity in education and research
Digital as a full-fledged alternative
Cyber security
Quality of education and research
Integrity and reliability of research
Quality assurance of education at underlying levels
Digital (open) educational resources
Innovative forms of education

**Figure 1: The HOSA objectives structure (higher resolution graphic in Annex B)**

This domain architecture for Identity and Access contributes to the realisation of virtually all objectives (orange) in the context of the ambitions of the sector (shown in green). Several objectives, such as 'Digital as a full-fledged alternative', 'Avoiding dependence on market players', 'Flexible learning paths', 'Modularisation of education' and 'More collaboration', are driving a different view of Identity and Access.

[1] Doelenstructuur van de HOSA | SURF.nl

# 2 Architectural vision

HOSA, thehigher education sector architecture, provides an architectural vision for the higher education sector with a horizon of roughly three to ten years. Various domains have been identified within HOSA, each of which further implements specific parts of the architectural vision. The architectural vision is based on initiatives and ambitions in the sector and developments in the market and society.

## 2.1 Introduction

Education and research in the higher education sector are undergoing a period of rapid change. On the one hand, we are witnessing global developments that impact the sector, such as ongoing digitalisation, different forms of national and international collaboration, citizen science, modular education and open research.On the other hand, change is happening due to advances in technology, such as the increasing use of the cloud, the rise of artificial intelligence, and new technology for reliably sharing identity and identity context data in a decentralised way.

The Netherlands has several ambitions that are facilitated by the higher education sector. Regions are joining forces with higher education institutions in the form of 'smart regions' to respond to these developments by focusing on smart technologies. In addition, the Dutch government has set out its ambition of creating a data-driven, knowledge-based economy, as detailed in the Knowledge and Innovation Covenant[2]. The Ministry of Education, Culture and Science formulated a number of goals with the sector in the strategic agenda. The emphasis here is on improving access to higher education, collaboration between institutions and with other parties, flexible higher education, better alignment with the labour market, alignment with society, regional integration and international collaboration. Alongside that, the independence of the higher education sector, the operational continuity of education and research, and the quality of education and research are key points for attention within the sector. Sector services as they currently stand are not in a position to achieve these goals and, in many cases, new sector services will be required.

Sector services that grant access to online services also need to be aligned in advance with the ambitions of the sector. Granting access needs to strike a balance between convenience on the one hand and protection from unauthorised access or unlawful use by untrusted third parties on the other. At present, the usual way of granting access is by means of a user name, password and possibly a token or two-factor verification. This is enabled by an entire infrastructure with associated process agreements operating in the background. Much of this infrastructure is organised along 'institution-centric' lines, while the trend in society and technology is to consider identity and access much more from the perspective of the individual. This demands that a different view be taken of these services for Identities and Access, as set out in the sections below.

**Education and research are changing**

In our sector, we are used to thinking from the perspective of students, lecturers and researchers. Students often implicitly assume that they and their studies will be based inside the walls of the institution. In the case of flexible education and lifelong learning, we can expect them to move beyond the walls of the institution and the timescale to shift from simply the duration of a study programme to something that is lifelong. This even though services for managing identities and access are currently organised within the institution, primarily for the duration of the relevant study programme. A mechanism is needed that ensures that the services keep pace with these developments, across all institutions and over a longer timescale.

The current situation is also largely built around study programmes. Greater flexibility and 'lifelong learning' means there will be a greater emphasis on enrolling for and following individual courses. The question then becomes, what precisely does the institution need to know about a student who only attends to follow one course and is enrolled for a full study programme elsewhere? Is it necessary for the student to present all their

[2] https://www.topsectoren.nl/innovatie/documenten/kamerstukken/2019/november/12-11-19/kic-2020-2023

personal data again as though they were enrolling for a full-time study programme? Or, is it sufficient for the person to indicate that they are a student at the University of Applied Sciences Leiden and that they are attending to follow one course? To what extent is it necessary to share additional data? In the current situation, there is a rigorous onboarding process for students and staff that places a significant burden on institutions. This process involves extensive verification of various details. For education to be more flexible and promote lifelong learning, there is a need for an accessible onboarding process that meets the needs of the participant while imposing less of an administrative burden on the organisation, with lower costs and better lead times. Alongside this, the onboarding process must be suitable for students from abroad.

In the field of research, the sector has set out its ambition to encourage increased involvement by society as a whole in research and its results. This could include companies, public bodies, citizens, hospitals and many others, who often come from abroad. This means that these parties need to be able to access research facilities, research results, etc. There are many aspects involved in the administration of accounts and access for all these parties. How do you know that someone is permitted to have access? And who administers the account and access? This requires a mechanism that enables you to grant access at a more granular level.

**Public values and big tech**

Institutions in the higher education sector provide education and carry out research. Public values play an important role in this. These values include equality, fairness, sustainability and privacy. These public values have come under increasing pressure in recent years due to the international tech giants exerting their influence. Students' privacy and the independence of education and research cannot be taken for granted and are threatened by these developments. For this and other reasons, institutions should remain as independent as possible from private market players.

It would seem to be an easy solution: if you want to enrol to study at an institution, you just log in with your Microsoft or Google account. These parties' platforms offer single sign-on and already have the systems and technology in place to provide much of the required functionality. They are also active across the higher education and research sector and have an attractive offering to make accessing education easier. The business model of these (usually non-European) players is often based on gaining insights into the behaviour of their millions of users. This model allows goals that are broadly accepted in society to be pursued (such as gaining insights into a pandemic or tracing missing people following a natural disaster). But, the flip side is that these insights are also used for commercial ends, such as targeted advertising, social profiling or political targeting, that are not acceptable to a growing group of users. The trend in Europe is towards a greater understanding that these developments threaten privacy. Once privacy is relinquished, there is no getting it back. Alongside this come issues of operational continuity: can the data stored on the platform of party X be easily accessed from the platform of party Y? Would institutions really still be able to access their critical education and research data if the contract with such a party were to be terminated?

**Public values and the individual**

In the current situation, we know who the students are and give them access to a range of facilities within the institutions or via the institutions that they need for their studies. Throughout their studies, all sorts of information is linked to the students, and profiles are gradually built up. Where is the student originally from? What are their prior qualifications? What route did the student take through the study programme? And, what were the results on completion of the course? This allows institutions to build up profiles for students during the time they are with the institution. There is a reason for building up profiles in this way, for instance to be able to support students better during their studies. Lifelong learning raises the question of how much information institutions should retain about their target groups. Unwanted traceability is a bigger issue in lifelong learning than with a four-year study programme. The personal profile built up during such a four-year study programme is already fairly detailed. In the case of lifelong learning, the student's profile will contain even more information. There is a risk that, without an explicit focus on privacy and security at the national level, a full profile will be created containing all the educational data of an individual, over which the person has little or no personal control. Addressing this problem is one of the objectives of this HOSA domain architecture.

Privacy is also of key importance within research. There are many stakeholders involved in a research project. For example, many research studies involve subjects who are willing to participate provided that their anonymity and privacy are protected. In addition, the results of research studies are often used by citizens, journalists, doctors and others, whose privacy also needs to be safeguarded. For example, third parties must not be able to obtain information about which persons have viewed what scientific content.

**Biometrics**

Relying solely on a valid login is not enough for some digital processes. Biometric features are often used directly or indirectly in the physical world for the purposes of highly reliable identification (such as whether or not you are the person shown in your passport photo). Many digital processes rely in part on the physical proximity of individuals or the implicit verification of biometric features. Applying for and issuing digital means of authentication often requires the physical presence of the person or an issuing process in which physical devices play a role.

In a fully digital world, some of these physical checks no longer apply. In the case of distance learning, or when enrolling for a study programme abroad, it is practically impossible to facilitate direct interaction. Using biometric features remotely would then provide a possible alternative. Biometric features are already used with mobile phones or to enable access to laptops. It would be tempting to extend this application to research and education processes that demand a high level of trust, particularly if national identity schemes cannot adequately assure a high level of trustworthiness (because there is no system in place, the system is not recognised, or there is no legal basis for its use).

However, due consideration must be given to the privacy and security consequences of the use of biometrics. Should biometric data get into the wrong hands it could have major, irreversible consequences for both the person and the security of organisations. Centralised systems that capture or use biometric data are fundamentally inappropriate for this purpose – both from a privacy and security perspective – because they come with far too great a risk. Solutions in which biometric features are managed and used on a person's own device do appear to be suitable for authentication, provided that the features themselves are not shared. One example is enabling a confidential key stored on your own device or in your own wallet. A rigorous assessment and decision framework also applies for these applications. Under this, processing biometric data is prohibited in principle, unless permission to do so is freely given or the use of biometrics is required for authentication or security purposes. A further point for consideration is the extent to which mobile device suppliers can ensure that biometric data remains within the device.

## 2.2 Three generations of IAM

An organisation, such as an institution or company, can issue a user name to a citizen or a customer. The organisation issuing such a user name is in a certain position of power towards the recipient. The public organisation or company may decide to revoke the user name or associated rights. This creates a high level of dependence on the organisation or company. In this arrangement, the person is not the owner of the identity and has little control over it, and the same goes for all data linked to this identity. A counter-movement is gaining ground globally by which the person creates their own identity and has personal control over which relationships with others this identity is used for. This concept is referred to as Self Sovereign Identity. In this system, the person will ideally have an identity that is independent of formal bodies of all types. Self Sovereign Identity is also referred to as the third generation of Identity and Access Management (IAM).

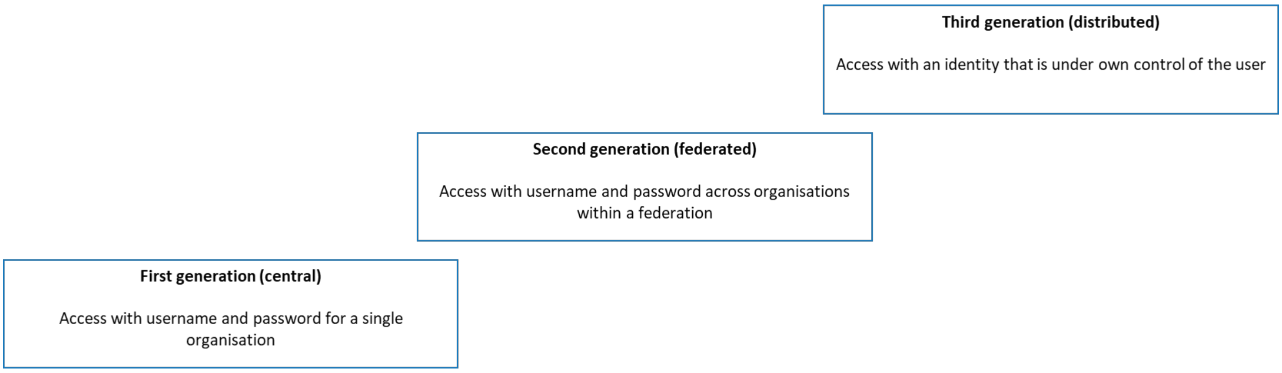

Third generation (distributed)
Access with an identity that is under own control of the user
Second generation (federated)
Access with username and password across organisations within a federation
First generation (central)
Access with username and password for a single organisation

Figure 2: Three generations of IAM

In a conventional setup, IAM services are based on the prior sharing of data for identification, authentication and authorisation (IAA) within the institution. This can be viewed as **first generation** IAM. The means of access, accounts and verification of access are issued and held in a centralised fashion all by the same party. The user will usually be identified separately for each institution, registered in a source at the institution, and this data will be shared with services the user wishes to access. The user has no knowledge and control over what specifically is done with the data. In the service (application), data is entered to enable authorisation within the service. The user is provided with login details to access the service.

Establishing federations of IAM systems between organisations can be viewed as **second generation** IAM. Organisations form mutual agreements to give their users access to one another's systems. In this case, the issuing of means of access and accounts is partly separate from access verification. The tech giants are offering solutions that allow users to log in to other service providers using Facebook, Google or other social media login buttons. Government agencies also offer citizens similar solutions to enable them to access their services, such as DigiD, the Dutch government authentication system. The organisations trust that their counterparts manage identities and accounts diligently, and on this basis grant these users access to services. A trust framework is usually employed for this purpose,facilitating sharing of data both in technical and legal terms. In the higher education sector, federation is in common use, e.g. through SURFconext and SRAM. The benefit is that users can access the same services with fewer accounts. The advantage for service providers is that they do not have to set up relatively costly processes for issuing and managing accounts themselves. The disadvantage is, that individuals are dependent on actors who are to a large extent able to track everything they do.. Undoubtedly, this is a major issue with commercial tech giants, posing a threat to public values.

The **third generation** of IAM is based on the concept of Self Sovereign Identity (SSI). In the ideal model, a person is the owner of their own identity, has control over where it is stored, and decides who to share that identity (or parts thereof) with. This system also allows for the option of withdrawing (revoking) another party's right to use the identity. The person is not dependent on a single central actor for their own identity. The system also applies principles of privacy-by-design, which means that the person cannot be tracked. This is because the issuer of the identity cannot see where the identity is being used to gain access. In the same way, the Dutch Ministry of Transport (RDW) and the municipal authorities do not know where and when an individual presents their physical driving licence in order to identify themselves. The HOSA IAM domain architecture assumes that it will become more commonplace over time for people to use Self Sovereign Identity in their day-to-day lives. We can therefore expect users of higher education sector services, such as lifelong learners, trial subjects or those interested in research, to use such services.

### Explanatory notes on SSI

SSI is the philosophy underpinning the third generation of IAM. Self Sovereign Identity allows data to be shared autonomously with a high degree of security. This technology also enables third generation IAM: Bring your own ID (ByoID).

In the first and second generations, the individual is highly dependent on another party who provides the identity and authentication means. These are 'centralised' models in which a few parties have control over how the whole system works. The identity and all features or attributes are held by the issuer or by the party that provides the authentication services. Not only that, they can – to a large extent – track what the person is doing with the identification means provided. If this party decides to stop providing the service or the person loses confidence in the party concerned, the person loses their associated identity and all related data, as well as the ability to authenticate themself to service providers who only use the means provided.

In the third generation SSI model, the roles are reversed. There are no parties involved other than the individual, who has exclusive control over how their identity information and related data is shared. The individual holds the necessary information themselves and decides whether or not to issue it to a service provider. This roughly the same as how things currently happen in the physical world: the relevant authority issues a passport or driving licence, but once these documents have been issued they are used independently by the holder. Credentials are critical to the SSI model. Credentials are evidentiary proofs that state certain facts about an entity, and can be used to prove these facts. The date of birth and the photograph on a passport can be used to demonstrate that the holder of the passport is an adult. The SSI model goes a step further in this respect, with the use of what is known as verifiable credentials. Real-time and non-repudiable checks can be made[3] on a credential to verify whether it was in fact issued by the issuer of the credential and whether this credential belongs to the person who presents it. In this way, verifiable credentials create a basis for trust in the digital world.

In the SSI model, the individual has a digital wallet in which they can keep digital ID cards they have received from other organisations and use them to demonstrate something, such as proof of membership, citizenship or skills. These ID cards (or the data on them) are often referred to as credentials. For example, the person can produce these cards at the point where identification is required if they are purchasing a service from an organisation.

Solutions using verifiable credentials come with a number of features that are distinctive from the physical credentials we are all familiar with. The first feature is that verifiable credentials are 'digital native', which means they can be used in situations where it is not convenient or not possible to use physical credentials. The second feature is that the model is set up from a privacy-by-design perspective. The organisation seeking proof will only receive evidence for the specific request, without any additional information that unnecessarily reveals more about the person's identity. For example, it might demonstrate that a person is over 18 years of age, but will not give their specific date of birth. This is not possible in the physical world using a passport: to demonstrate that you are over 18, you have to show your date of birth on a document that also contains a lot of other information.

The third feature is direct digital verifiability. The response to the request will also indicate the authority that issued the credential, including the digital signature of that authority. This allows the organisation to check whether this declaration was in fact issued by this body, without the need to consult the issuer of the credential. Consequently, there is no way the issuer can build up a profile of the person.

Verifiable credentials are not just suitable for use by individuals. Organisations, animals, systems, natural objects and things made by people can also have a digital identity, expressed as credentials[4]. This would allow a much more equitable situation to develop in digital processes between organisations and individuals than is currently the case. Both the organisation and the individual would have to identify themselves to one another,

[3] The difference between this and physical credentials is the non-repudiability. A passport contains a whole range of security features, but only some of them can be verified in real time.

[4] Unlike 'persons', these entities are of course not 'self-sovereign' in the strict sense of the word. However, this does not detract from the ability to link credentials to these entities. This is discussed in greater detail in Section 5.

allowing a situation of mutual trust to take shape in a digital world. This stands in contrast to the situation at present where the person logs in to a website but may find it difficult to determine whether the organisation is trustworthy. Individuals need to be able to check whether a site that presents itself as a 'scientific' or 'public sector' website is in fact trustworthy. And, the organisation may want to be able to check that the person logging in is in fact a person and not a robot or AI software. Many websites currently use Captcha where the user has to carry out a task that is easy for a human but very complicated for a robot (for example, you may be asked to select all the pictures in a grid containing traffic lights). This process could be made more user-friendly and reliable if a digitally trustworthy statement 'I am a human' could be submitted.

**Will SSI end up being used for everything?**

It is likely that first, second and third generation solutions will co-exist over the next 10 years or so. A crucial aspect of SSI is that it supports a change in the approach to how identity is managed for businesses, users and government bodies, paving the way for a redesign of existing business processes.

Everyone needs to be able to obtain services from the higher education and research sector. This means that basic services must be easily accessible, but also secure for everyone in society to use. Examples include viewing particular research topics, using open data and publications, learning about education or watching information videos. The ideal situation would be where individuals are able to easily access education and research services in the sector using their own Self Sovereign Identity, such that they do not have to reveal more privacy-sensitive data than is strictly necessary. This would allow trust and security to be created while preserving privacy and public values.

Based on public values, it is desirable that options for studying and collaboration across institutions should be set up without these parties having to share large amounts of data. For this reason, the philosophy and principles underpinning SSI are taken as leading in this domain architecture. Alongside the technical aspects, institutions also need to consider that this will involve organisational change: from a situation where only the organisation's own employees and students can use their facilities and services, with the identities and means of access specific to that institution (first and second generation IAM), to a situation where third parties and more and more employees and students take their personal identity and means of access with them. The term Bring Your Own ID is used here, or the abbreviation BYOID.

Alongside this, it is critical to make a distinction between the use of data in the context of IAM and the application of data in actual business processes. Much of the data required to provide services and education will continue to be held in the institutions' information systems. In addition to interactions where a natural person is directly involved (in the form of their 'digital agent', e.g. a wallet), direct interactions between data sources and data users will continue to take place. In both scenarios (via an agent or directly), it is necessary to provide transparency about data use including the lawfulness of its use**.**

## 2.3 Application to the higher education sector

There are a number of developments in our own sector already moving in the direction of Self Sovereign Identity concepts. Examples include EduMIJ, microcredentials and EduID. EduMIJ is a concept in which students are given a wallet that they can use to provide potential employers with proof of a completed study programme or courses. Microcredentials are formally obtained credits (ECs) for courses a student has already completed as part of their education. Students can use these as evidence for exemptions. EduID provides a form of identification that people can create and manage for themselves. Specific evidentiary proof can be linked to this, such as the fact that you are working or studying at a higher education institution. At present, it is used for guests, edubadges and a student mobility pilot, but EduID can also be upgraded to provide identification for use across higher education.

SSI also provides the potential to reshape collaboration between organisations. Just as a person can decide for themselves the parties from and to which they display a credential, so institutions can decide for themselves who they provide the credential to and what criteria the individual must satisfy in order to receive a credential, and institutions can decide for themselves which credentials from which parties are sufficiently trustworthy. This approach offers the requisite flexibility to grant access to certain services for different parties, many of whom will be from outside the organisation. This also allows institutions to retain control over who they give access to and under what conditions.

However, the granularity offered by verifiable credentials does come with the risk of increasing complexity for the person. With this system, the user has a wallet with potentially a multitude of credentials, and service providers may require all sorts of different evidentiary proof. Thinking in terms of a conceptual[5] *digital* higher education card helps to make this clearer. A higher education card is in fact a verifiable credential set issued by an organisation within the sector with the aim of organising access to online or other services in an efficient manner. The higher education card would hold most of the required evidentiary proof, making it convenient. Comparable examples in the physical world include student cards, campus cards and employee IDs. You can display it just as you would a driving licence to access a particular service or place. The digital higher education card contains a set of data that is a digital representation of an entity within the higher education sector. This entity can present different sets of data for different situations[6]. For example, the higher education card for researchers might be different from that for students.

In the desired situation, each individual who enters into a broader or more formal relationship within the sector will receive a digital higher education card. This will allow the person to digitally identify themselves and gain access to digital services within the sector and potentially elsewhere. The person can use or hide the verifiable claims on the higher education card in a transaction with a third party at their own discretion. For example, the claim that they are enrolled for a course. Claims from organisations outside the sector can also be included on the higher education card. Work still needs to be done to determine who should and should not get a higher education card. However, an example might be that a person considering open education out of personal interest only would not receive a higher education card, but if the person indicates that they want to obtain a microcredential for one study module then they should receive a card.

A higher education card trust framework would be established to allow recipients or service providers to determine the degree of trust they can place in the higher education card. The trustworthiness of the higher education card is defined by the degree of assurance established in the user identification, the authentication means and the attributes. For example, a service provider who wants certainty when making a decision, such as granting access to a particular online service or issuing a diploma, needs data that is valid for the relevant type of decision. The criteria used by the service provider for this purpose can and should be determined by the service provider itself. It is complicated, because how do you know whether the data is sufficiently trustworthy? To meet the needs of service providers, a trust framework will be set up to make it easier for them to determine the validity of data shared under such a framework, as required to have certainty about a decision.

A person can hold several roles simultaneously or consecutively. For instance, someone could be a student, research student (work placement or graduation project) and an employee (student assistant) all at the same time. Throughout their life and career, a person may change roles or be temporarily assigned an additional role. One example would be an employee of a company who is involved in a research project at a higher education institution. The sector services of the future need to be able to enable such persons to have the credentials that fit their roles at that time and to use the associated credentials. For example, a researcher

[5] Conceptual, because it cannot be assumed that a digital higher education card will be rolled out as a separate digital object in its own right. The intended functionality is more likely to find expression in a set of agreements within the (international) higher education sector in which the institutions concerned recognise and acknowledge the credentials issued by or on behalf of other institutions.

[6] In the VC data model, the term 'persona' is used here, meaning that part of the full identity that a subject wishes to present in a specific context.

who spends a certain time at an institution should be able to take verifiable proof of publications published under their own name, but which are held in an institutional wallet, with them. A verifiable credential (unless revoked) should then be transferred to this individual's own wallet. It follows from this that the form of the credentials should not be dependent on the chosen wallet, and that there should be interoperability and portability between wallets.

In the desired situation, the higher education card would work in combination with other authentication means used when issuing credentials or when using credentials for digital services to verify that someone really is the person they are claiming to be. In most cases, this will not be necessary and the higher education card will be sufficient for authentication. For example, an additional identity check might be required – by means of a (digital) ID card or passport – when sitting an examination.

The HOSA IAM domain architecture is not limited to natural persons in the higher education sector. Natural objects or things made by people also increasingly need a solution to allow them to be identified and to be able to present specific proof. Examples include websites that need to be able to prove that they are trustworthy and not phishing sites, datasets or publications that need to demonstrate their authenticity, or parts of IoT networks used for research that need to be able to identify themselves. While such developments may seem a long way off from our present viewpoint, if there is a change in the paradigm, the principles underpinning the technology will need to allow for this.

## 2.4 The maturity of the technology and initiatives

Paradigm change is not possible without mature technology. However, the interests of privacy and public values are so significant that this domain architecture already looks to these in the vision and the underlying models.

SSI is still at the development stage and standards have not yet been crystallised. It will take another two to five years for large-scale application to start to become reality. The majority of the associated technology concepts, such as distributed computing and cryptography, have been around for years and are now mature technologies. The complexity partly lies in how the technologies interface with one another.

SSI uses Distributed Ledger Technology (DLT) in many of its current implementations. Blockchain is a common element in the architecture of SSI solutions. The use of distributed ledger technology such as blockchain is relatively new, with crypto currencies like Bitcoin being the best known application. The use of blockchain as a key element in SSI is not beyond question. Research firm Gartner expects the technology to reach a state of maturity between 2023 and 2025, at which point broad adoption will take place. Similar signals from NIST indicate that blockchain-based identity could become a fundamental architectural component in the internet of tomorrow, but that aspects such as scalability, security and privacy all need to be successfully translated into solutions.

The W3C standards for verifiable credentials do not set out precisely how solutions should be realised in technical terms. It would be perfectly possible to implement an SSI infrastructure without blockchain or other form of distributed ledger. The underlying inter-connected technologies for SSI are not all fully mature at the moment, to the extent they can be widely deployed in the sector. There are still issues to be addressed around revoking credentials, for example, and options for logging in when you are offline. Similarly, user applications are not currently set up to handle just-in-time provisioning.

However, there are various indicators that broad investments are being made to make this technology suitable for wide application. The tech giants are in the process of developing solutions and many suppliers are coming out with wallets. At present, these are separate initiatives resulting in a whole range of different wallets and protocols. Organisations such as SOVRIN, ToIP, DIF and the OpenID Foundation are developing models, technology and best practices. Alongside this, global standardisation organisations such as W3C and NIST are in the process of defining and detailing the necessary standards. However, this is a slow process and the required protocols in particular have not yet been standardised. In the Netherlands, TNO, DUO and SURF have acquired some initial experience in an experimental environment. Under pressure from the EU and other initiatives on wallets and European identity, it is anticipated that convergence will take place leading to applicable and coherent agreement frameworks.

At the same time, it is clear that promising developments to enable greater flexibility in the sector, such as microcredentials and open badges, are also underway without the necessity for a full SSI infrastructure. There is no need to wait, but it is necessary to work out how the developments can be linked together and be related to one another.

Several initiatives are taking place in the US, such as Sovrin. Sovrin could become a tool for IAM services that could be used to provide self sovereign identities globally. Companies and government bodies all over the world would be able to use this service for a fee. However, there is a risk of Europe becoming too dependent on the US. An identity infrastructure can be regarded as a utility or critical infrastructure within the country. This has been recognised in Europe and initiatives have emerged to create identity services specifically for Europe.

The EU and the Dutch government are investing in identity infrastructures that place core values, such as privacy, autonomy and cross-border usability, at the forefront. This is reflected in proposals for an updated legal framework in the form of (amended) legislation and regulations, such as eIDAS and the Dutch Digital government Act (wet Digitale Overheid). In parallel, programmes and pilots are being launched to explore the (technical) feasibility of credentials, wallets and data management.

In its vision of digital source identity, the Dutch government sees itself as holding a critical position of trust as the 'issuer' of digital source identity (DBI) for citizens, similar to its role in issuing passports and identity documents. This view could be in conflict with the concept of SSI, due to the risk of digital identities being issued exclusively by a central actor. The SSI model makes clear that it is not necessary for identity information to be issued from a central source. The Dutch government acting as an 'issuer' of credentials regarding a citizen's identity fits perfectly within the concept of SSI, and may be advantageous for use in situations where a high level of trust is required[7]. In that case, it would be possible to link the higher education card and the digital source identity together. Examples where this might apply include enrolling for a course of study or issuing a diploma. In the case of processes where this is not required, it must be possible to use other identities from other issuers. Furthermore, this is necessary to prevent the risk of the unwanted correlation of personal data and the unwanted tracking of individuals.

It is important for the sector to follow these developments closely and to align with them. This means the sector will not have to develop all the infrastructure and technology itself, but can share expertise from national and international organisations and benefit from initiatives like IRMA. This will allow the sector to concentrate on the criteria it wants to place on wallets and how to organise the issuing of credentials in a way that can be used widely.

[7] However, consideration must be give to a situation in which a substantial part of the population in higher education does not have Dutch or even European nationality.

# 3 Use cases

To demonstrate how IAM would work in relation to the intended methodology, a number of examples for education and research have been outlined in the form of various use cases. Terms are sometimes used within these descriptions that have a specific definition within particular disciplines. The purpose of the use cases is not to describe the higher-level business process correctly in every detail, but to make clear how verifiable credentials and a decentralised identity could play a role in this situation. For the same reason, the use cases do not cover all possible variations. The use cases also demonstrate that it is not just people that can be holders of identities with specific roles and attributes, but that this could also apply to services, devices and data provided by organisations.

## 3.1 Education use cases

**Use case: Getting information about education**

An individual is interested in a particular study programme. This might be following a visit to an education fair or an educational choices website. As a result, they want to stay in touch with an education provider. The person does not want to enter into an in-depth relationship at this time, but just wants to find out a bit more about the education provider. The person would prefer to remain anonymous as far as possible. They are happy to receive updates from the institution now and again with relevant information. They have the information required to do so, but do not expect to have to provide their address details, age and other personal data just to stay in touch at this basic level.

This can be done using SSI. The individual has a wallet in which their contact details are stored as a credential, along with other data. Using a smartphone, the person scans the QR code shown in the education provider's information environment (e.g. an exhibition stand or a page on an educational choices website). The QR code links to a website that initiates a session with the personal wallet. After the person logs in to their wallet, a dialogue takes place in which a minimum set of contact details (email address or telephone number) is requested. The intended purpose of 'receive course information' is clearly indicated as part of the dialogue. If the individual is in agreement, they can give their consent to the intended use and duration of use. The institution now has validated contact information and confirms this via the contact address provided.

If the person does not have a wallet, the dialogue will take place on the education provider's website. Since the contact details do not come from a verified source, an extra step will be required, for example confirmation of the email address before information is sent.

As is the case when communicating with a bank, it will also be important for individuals to have certainty that they are dealing with a real university or college. This will ensure the person knows that they are dealing with a trustworthy institution and not a phishing site where criminals pose as an institution. A properly implemented infrastructure for processing verifiable credentials would facilitate these checks and so provide the basis for mutual trust.

Technical:

An individual can use a digital wallet to collect data from different (trusted) sources. This data can be presented/submitted upon request. The person can choose which information from the wallet to present. So, if they are asked for an email address, the person can choose which address from their trusted data in the wallet to submit.

Various methods are available for the mutual sharing of credentials, e.g. based on DLTs or using peer DIDs (and associated DIDComms).

**Use case: Taking a single course**

The person has gone through their own information-gathering process and wants to follow a single course at a highereducation institution.. This institution aims to provide easy access to individual courses and, for this reason, only asks for details from the applicant at the time it becomes necessary. This institution offers those interested in the course the opportunity to view the study material online first. This is all in the pursuit of open education.

The person logs in via the online catalogue using a code they received at an education fair. This creates a direct link to the institution and means the person is already known to the institution to a certain extent. The person is sent a link giving them direct access to the course in the institution's digital learning environment. The person decides after readingthe study material to take the course.

The course starts with a number of online lectures. An advance payment is required to be able to access these. The person clicks on a button to follow the first set of online lectures and pay for them. They pay from their study credits via the national infrastructure. The person is given a receipt in the form of a proof of payment credential. They present the credential from their digital wallet in the digital learning environment of the institution and are given access to the online lectures.

The person would like to obtain the certificate for the course and decides to sit the examination. The institution wants to have certainty about who is sitting the examination. In this case, a higher level of assurance is required. The person is asked to submit a credential that identifies them with a higher degree of assurance, for example using authentication that is linked to their national source identity. This allows the institution to link the results of the check to the individual with a high level of assurance.

After passing the examination and satisfying all the requirements, the person is awarded the certificate. The institution issues the certificate in the form of a verifiable microcredential. The person can then use this to demonstrate to third parties that they have completed the course.

Technical:

An individual can use a digital wallet to collect data from different (trusted) sources. This data can be presented upon request. The person can choose which information from the wallet to present. If asked for official proof of identity, the person can choose which type of ID in their digital wallet to use. As part of this, the results are issued to the person associated with the credential concerned. So, a different identity document could potentially be used in a later process.

If someone holds several nationalities, there will be several issuers of national identity documents. These can be included as separate credentials. It is up to the holder to choose which of these they wish to use and to the verifier to make clear which of these can be accepted.

**Use case: Onboarding for a study programme in higher education**

The person has successfully obtained their entrance diploma for higher education and wishes to enrol for a study programme at an education institution. In the current situation, they would do this via Studielink. This system is used partly to reduce the administration costs of onboarding, which would be significant if managed separately by each institution. A number of checks are carried out in the current process. Using verifiable credentials would allow these checks to be carried out more efficiently and may result in full digitalisation of the process. This would however require using a national sector service, such as Studielink.

In the current situation, the institution requests information from Studielink, such as the preferred name, email address and phone number. In the desired situation, this data could be issued to the person as credentials using an SSI infrastructure, and then this person can consciously choose to issue the data to the institution.

During the onboarding process, the person will be asked whether they already have a higher education card. The higher education card holds a number of identifying attributes and verifiable credentials that the person can present in the context of the higher education sector or elsewhere[8]. For example, it could be used as proof that the person is a student or that this individual has completed particular courses. The higher education card enables the holder to provide only the data needed for onboarding. For example, the person could show proof that they are a student without divulging their citizen service number or the name of the study programme or institution, if that is not needed[9].

If the person does not have a higher education card yet, one can be created in the online sector service. At this time, the person can indicate the digital identity they want to link to the higher education card. A government provideddigital source identitycould be used for this purpose, or any other trusted identity scheme. These links are only known to the individual concerned and will not be divulged unnecessarily.

Various other aspects arechecked as part of this process, such as a request for details of the applicant's previous education. In due course, a verifiable credential will become available that can be submitted at this time. A further example is where foreign students need to be able to demonstrate that they have an adequate proficiency of Dutch (e.g. at level CEFR B2). In time, the individual will have the ability to submit a verifiable CEFR credential, potentially in the form of a microcredential as already widely used in the sector. Nuffic, the Dutch organisation for internationalisation in education, would also be able to issue verifiable credentials on the parity of foreign study programmes that individuals can then use in the enrolment process. One characteristic of these verifiable credentials is that the parties requesting them, such as Studielink, can check whether the credentials were actually issued and have not been revoked. This should be done without Nuffic or any other issuer being aware that this verification has taken place. To assure this, the process applies the principles of privacy-by-design, with only data relevant to the intended purpose of processing being shared.

The digital enrolment process at the education institution allows for the individual's identity to be uniquely verified. If the verification process is successful, the institution can enrol the person as a student. The verifiable credential of the study programme will now be linked to the student's higher education card, allowing the person to add the claim that they are enrolled in the relevant programme at the education institution.

A person wants to return to education and follow a course of study while continuing in employment. The person still holds a higher education card and the credentials linked to it. The sector services have a facility to enable the person to re-connect their national identity to the higher education identity. The person enrols for the study programme as described above. As part of this process, they inform the institution of specific details on their higher education card via the national sector service. The institution can be confident that the credentials for the completed course of study are still valid.

[8] In terms of the Verifiable Credentials data model, the higher education card therefore represents the 'higher education persona' that forms part of the full identity that a person can divulge to identify themselves in the higher education sector.

[9] A citizen service number will soon be required under current legislation, and Studielink will be obliged to ask for it because of the link with DUO and various legal verification processes.

Technical:

An individual can use a digital wallet to collect data from different (trusted) sources. Data relating to education and research in the higher education sector is issued in the form of verifiable credentials that can be imported into various wallets. The wallets can then be used to present a selection of attributes from the credentials to a verifier as a verifiable presentation. The presentations only contain the information that is necessary and that the holder wishes to provide. This allows a tailored set of attributes to be submitted depending on the verifier. This could come into play in other situations where an individual needs to prove they are still actively enrolled as a student, such as to demonstrate that they are legally entitled to rent student accommodation. In this case, only limited personal data needs to be shared and a credential can be presented periodically that proves the individual's current student status.

**Use case: An international student wants to find out whether a Dutch study programme is accredited**

An international student attending a foreign education fair needs to know whether a study programme is accredited by the Dutch government. An SSI infrastructure can help in this case, since the student can query the official status of the course of study via a verifiable credential for thatcourse of study. Formal products in the higher education sector, such as study programmes, can be regarded as a subject to which the credentials relate.

The international student uses a QR code available on the stand at the fair to access these credentials. The Dutch institution asks for some credentials from the international student, and the international student asks for some credentials from the institution. The institution now knows that it is dealing with a real person, without this individual having to relinquish all of their privacy. The international student can have assurance that this is a trustworthy institution that exists in reality.

After making this connection, the international student uses the institution's service to query whether a study programme is accredited. The chatbot asks which specific study programme the student is enquiring about, and provides proof that the programme is in fact accredited. This proof contains a key that the 'agent' (e.g. app on smartphone) of the international student can use to check in the background whether the proof shown is genuine according to its issuer.

The issuer of the proof presented by the institution is a government body (in this example, NVAO[10]). The government body has made the proof available to the institution and signed it. In addition, the proof has been published in a public register (e.g. maintained by DUO, the government education agency) that shows this proof has actually been issued. The agent of the international student checks whether the proof for the course of study that they wish to follow has actually been issued. It is apparent that this is the case, and therefore proof that the study programme is accredited has been provided.

**Use case: Student living close to a different campus**

It is difficult to find student accommodation in the city where a student is pursuing his or her studies. The student has found a room elsewhere that is within walking distance of the campus of another institution. This institution offers a large number of individual courses andhas good facilities for people who are not enrolled for a full course of study there.

[10] Nederlands-Vlaamse Accreditatieorganisatie [Dutch-Flemish accreditation organisation]

The student enjoys studying in an environment with others and therefore would like to use the facilities of the campus that is within walking distance. In order to allow the studentto usethese facilities, the institution needs proof that this person is a student in the Netherlands. The student scans a QR code on the campus that takes them to an online portal. The student uses some details from the digital higher education card stored in their wallet to demonstrate that they are studying at the other institution in the Netherlands. This is automatically verified in the background. Following this authentication process, the student will be able to book a carrel and use the library and other services.

After a couple of months, the student completes the first modules in their study programme. The chosen programme has a relatively fixed curriculum with the opportunity for students to choose modules themselves at various points. In the upcoming period, the study programme has options in the curriculum to enrol for additional modules, including at other institutions. The student has now experienced the campus and knows a bit more about the institution that is within walking distance.

They decide to enrol for a module with this institution. The student logs in to the institution using their own higher education card. A digital verification is carried out to verify that the claims relating to the student's status are correct. If the verification is OK, the student is issued a digital identity as a guest student at the second institution and a relevant credential is linked to the wallet. On the basis of their identity as a guest student on the higher education card, the student can now select a course to follow. The student can then access the course based on the digital identity as a guest student.

Technical:

For the phase in which the student is using the facilities on the campus of the other institution as a guest student, there is no need to share information from the source systems of the home institution. All the necessary information can be provided at that time as a credential or presentation by the student. Any additional attributes that the host institution needs (such as a phone number or email address) can also be provided directly from the wallet.

When the student enrols with the other institution, information needs to be shared with the student's main institution. Keys are provided by the student for this purpose and, on giving their consent, these can be used to allow the two institutions to share information. This information will be used to decide how to deduct study credits (see below).

**Use case: Lifelong Learning (LLO)**

A professional person graduated 15 years ago and has been working in business ever since. This person has completed several course modules over the past six years and received microcredentials for them. These microcredentials are held in their personal wallet. The person is wondering whether all of the completed course modules would add up to a diploma, and which modules would still be required to complete before getting a diploma.

The institution, which offers modular education, has an app that allows students to check what the need before obtaining their diploma from the institution. The professional downloads the app and starts a dialogue. It is an easy matter to provide the requested credentials using the data in her personal wallet. No privacy-sensitive data needs to be provided; the claim that all microcredentials are linked to the same person is sufficient.

The app indicates that there is a reasonable match with a particular study programme and indicates an approximate number of course modules and hours remaining based on the set of modules shown. The app asks if the person wants to schedule a meeting with a study coach. After the meeting, a recommendation is made to which the professional agrees. The study coach sends the recommendation and the collected microcredentials digitally to the examinations board for the relevant study programme. The board is in agreement and the secretary of the board generates a digital letter of admission for the programme, together with the relevant exemptions in the form of verifiable credentials.

The individual goes to the national sector enrolment service to enrol for the study programme concerned. This service identifies the person using the details on her higher education card. The person can use the digital letter of admission to demonstrate that the institution has agreed to her enrolment. The sector enrolment service can then support the person in the next stages of the process to formalise her enrolment.

**Use case: Demonstrating required qualifications**

When communicating with companies and the authorities, a person may be asked for verifiable proof of a diploma or course modules they have completed. This could be the case when applying for a job or a permit. The person has a wallet in which they hold details of diplomas for study programmes and microcredentials for course modules. The relevant attributes can be provided from the wallet as a verifiable credential. The SSI infrastructure allows the recipient to verify the claim. The issuing institution is not notified when a third party verifies a credential, so privacy of the person is ensured.

**Use case: Using study credits**

A professional person registers for a course. He meets all the prior education requirements and has also successfully passed the preselection. He can start the course as soon as it has been paid for. The government has given him a lifelong learning budget that entitles him to take a single course. This entitlement is stored in his wallet in the form of a credential ('single course credit'). He presents this credential to the educational institution. It verifies whether the credential can be used for the chosen course and whether it is still valid (not used previously and not expired). Providing it is valid, the professional can go ahead and start the course.
NB: The exact implementation of the financial business processes related to this use case is outside the scope of the IAM domain. A number of payment methods are available (bank transfer, direct settlement with study credits, redemption of a study budget, one-time voucher, pre-paid tuition fees, settlement through employer's study budget) and various mechanisms for settling payment between institutions (via a central party, by means of bilateral agreements, etc.) It is also important to think carefully about where records of study credits would be kept. In any event, a (trusted) intermediary ('clearing house') with strong privacy arrangements is needed to administer study credits.

## 3.2 Research use cases

**Citizen wishing to participate in research as a trial subject**

The news has a report about a research study looking for trial subjects. Those who are interested in participating should go to a website to register. Someone who is interested looks up the website and verifies that it is trustworthy, partly by checking that it has trustworthy verifiable credentials. The SSI infrastructure supports this by allowing the party behind the website to be verified.

The website shows general information about this research study and has a digital certificate that demonstrates to interested parties that it is an officially accredited research project. In this case, a credential is shown that is issued by the Dutch Research Council (NWO). The interested party is familiar with NWO and concludes that this is a trustworthy research project.

The interested person decides to register. The website then asks for some details that can be provided using credentials from the person's wallet. It is sufficient for this research study to receive a 21+ declaration and a unique person key to ensure that the same person cannot use different ID cards (such as a bank card, driving licence, etc.) to register as a trial subject multiple times. The person does not need to state their actual age to demonstrate that they are older than twenty one. In this case, a credential can be used only indicating that the person is older than twenty-one, signed by the body that vouches for this.

Even though the research is anonymous, the person interested in being a subject indicates that they would like to receive information about the results of the research. To do so, they can leave verified contact details from their wallet. The research institution will ensure that the contact details and consent to use the information provided are kept strictly separate from the actual research data. At the end of the research, the results will be shared with the interested party. Since the research data has been kept separate from the contact details at all times, this can take place without establishing any link between interested parties and the research data they supplied.

**Citizen scientist wishingtoto usedata and facilities**

Many volunteers contribute to research by engaging in various activities. In the desired situation, sector services also need to allow for this. A person is active as an amateur meteorologist in their spare time. The individual would like to join a European network in which amateurs contribute with data from their own weather stations. The amateur meteorologist wants to use data and weather models available via the European network to configure their own weather station in the role of citizen scientist.

The person initially identifies theirself as a citizen scientist. The network of researchers asks the participant for details of their prior knowledge in this field. The individual presents a verifiable credential of a course in meteorology completed some years ago. To complete the intake process, the individual agrees to the conditions of use of the data and models. The citizen scientist is now admitted to the network.

The person then informs the network of the meteorological equipment they are using. The facilities that form part of the network will also have their own identity (more than just a unique serial number), so that the various citizen scientists can have confidence they are working with correctly calibratedand accredited equipment. Compliance with these quality criteria can be demonstrated on the basis of verifiable credentials. This allows the person's weather station to be included in the monitoring network and the data from that weather station to be included in the network's datasets. This contributes to creating a reliable system of equipment with reliable data for research. The maximum validity of the credential can also be indicated to allow checks to be made periodically to ensure that the equipment is still satisfactory.

**Student using facilities for a dissertation**

When producing their dissertation, a student wants to use various facilities available for their area of research. In order to use these facilities, the student must be able to demonstrate that they are working on a related study or that they are involved in the research study as an employee.

When the student seeks to access such a research facility, the facility asks for proof that the student is enrolled on a course of study in a relevant field. For example, for access to a medical database the facility will ask whether the student is enrolled on a course of study in healthcare. The student can select this proof once from the set of claims included in the student's wallet from their course enrolment. Each subsequent time the student accesses the database, this proof can be shown by the system the student uses to access the database. It is important here that the credential 'enrolled on a course of study' has a finite validity period.

**Full-time researcher**

An individual has successfully completed a course of study and continues to work full-time as a researcher at a higher education institution. This person did a graduation research project and, in the role of a student researcher, had access to a number of digital research environments at the institution and a number of partner institutions. The person now enters employment with the institution and receives a credential for this purpose that shows that he or she is now an employee. In order to continue to work directly in the digital research environment using the profiles already held for the person as a student, the individual can provide the verifiable credentials from their student data and the profiles can be linked within the research facility. The person is informed that their study rights are being terminated as they will no longer be enrolled as a student, but that their proof of identity as a student in the past can still be requested and demonstrated.

The researcher works for a number of years and then has a publication ready in draft form. He or she reports this to an open science publisher who arranges for an independent peer review. After completion of the review process, the researcher signs off the end result and the reviewers (anonymously) sign to confirm that their comments have been correctly implemented. A representative of the institution also signs off the end result for publication. The open science publisher verifies that all parties have digitally signed the publication and verifies that they have valid credentials. The publisher then generates a final version with the associated timestamps and credentials. All and sundry are now able to check that various trustworthy organisations vouch for the quality and authenticity of this publication. The researcher then receives a verifiable credential that proves that they are the author of the scientific publication, and the institution receives a verifiable credential that the research was carried out within that institution.

After many years of employment, the researcher leaves the institution. Questions and requests continue to be received about the researcher's previous publications. The researcher wishes to continue to answer such questions after the end of their career in research. The researcher holds a research identity that can be linked to the publication in an SSI infrastructure. During the course of their career, communication facilities made available by the institution had to be used, including a wallet selected by the institution. After retirement, the researcher changes the contact attributes associated with his/her research identity so that they can still be contacted, now in the capacity of a private person. Because the research identity itself does not change, the credentials issued to prove copyright do not need to change.

Technical:

The researcher uses a research identity that is independent of the institution (similar to ORCID[11]). Relevant verifiable credentials could, for example, be credentials for research articles, awards conferred and datasets, and are linked to an open identifier schema such as ORCID, meaning that they remain usable unless and until the researcher changes their ID.
Contact details associated with that ID can be changed. It is important to be able to safeguard the researcher's privacy in this situation. New functionality may need to be developed within ORCID or an equivalent scheme for this purpose.

If a specific higher education wallet was used, the credentials can be transferred to a personal wallet using defined transport mechanisms for transferring credentials between wallets.

**Sharing data with an unknown scientist**

A full-time researcher at a research university has built up a large dataset together with colleagues over the past few years. They can see that there is a lot of demand for the specific data they have collected. However, the Dutch government has designated the dataset as *confidential*. This means that research data may be used by research institutions, but must not be unintentionally shared outside the EU.

The researcher's university is connected to the RDM infrastructure as described by HOSA. Parties that are affiliated can share datasets with other parties or give other parties access to the datasets if the data

[11] Open Researcher and Contributor ID

cannot or may not be moved. Requests to share data are sent to the research groups that have authority over this data.

The researcher has received a request to share the dataset. As part of the online intake process, the requester was requested to show a number of verifiable credentials. The first credential requested is to demonstrate that the applicant works at a recognised research institution. This credential is provided and rigorously verified via the issuer of the credential. The second check relates to the question of whether the research institution is accredited to process confidential research data at the required level. This is also demonstrated. The final verification of the supplied credentials relates to whether the applicant is a researcher authorised by their own organisation to work with confidential data and that this authorisation has not been revoked.

The researcher does not know the applicant, but has sufficient confidence as a result of the credentials shown in context to grant access to the dataset. The researcher presses the button to allow the request. The researcher then contacts the applicant personally to discuss how to interpret the data.

## 3.3 Use cases from the perspective of the institution

Employees of an institution often have a role in which, rather than representing themselves, they represent the institution. The higher education card of the institution can be used when communicating with services used by employees. This means that the institution also has an identity. The institution has a (company) wallet to allow for data associated with the identity to be managed. This provides functionality for various institution credentials to be held, such as general contact details and its accreditation status as an education institution.

For example, a number of employees within the institution may be authorised to use the higher education card of the institution. The institution has (human or automated) employees that are authorised to grant these authorisations to specific employees. These employees can hold these credentials in their wallet. The employer may impose additional requirements on a wallet or make a wallet available to an employee to receive, manage and share work-related credentials.

It must also be possible for a person outside the institution to check data issued from an institutional higher education card for its trustworthiness. The person can check with an agency of the Dutch government, e.g. DUO, whether the institution is in fact trustworthy. As the issuer of these credentials, DUO can sign the proof and ensure that the public part of it is included in a registry. This allows the individual to check that the credentials have in fact been issued by DUO and that the credential has not been revoked. After this check, the person can have certainty about whether they are dealing with a trustworthy institution. This entire process takes just a couple of seconds.

# 4 Organisational architecture

The use cases give examples of how SSI and verifiable credentials could work in the higher education and research sector. A number of concepts have emerged in the course of detailing the use cases. These are described in the section below showing how they relate to one another. It is structured around the specification for the Verifiable Credentials data model from the W3C[12].

**What is a verifiable credential?**

The term credential already exists in the non-digital world (identity cards, means of payment, diplomas, mortgage deeds), where it may refer to the following:

- Information related to the identification of a subject (e.g. a photograph, a name or an identifying number)
- Information related to the issuing authority (e.g. a municipality, a public body or a certification authority)
- Information related to the nature of the credential (e.g. a Dutch passport, an American driving licence or a health insurance card)
- Information related to specific attributes or characteristics confirmed by the issuer (e.g. nationality, driving licence or date of birth)
- Evidence regarding the source of the credential
- Information related to restrictions on the credential (e.g. expiry date or conditions of use)

A verifiable credential is the digital version of an 'analogue' credential, and can contain all the information held on its analogue counterpart. When used in combination with technology like digital signatures, verifiable credentials can be more tamper-proof and more trustworthy than their physical counterparts, and because they are digital they are innately portable and verifiable.

## 4.1 Overview of the ecosystem

In the use cases, people, organisations and things hold different roles. The W3C specification introduces the following roles[13]:

- ***Holder*** – the role played by an entity in possessing one or more verifiable credentials and generating one or several verifiable presentations. Examples of *holders* include students, employees and customers.
- ***Issuer*** – the role played by an entity in making claims about one or more *subjects.*
- ***Subject*** – an entity to which claims relate. Examples include people, animals and things. In many cases, the holder of a verifiable credential is the *subject*, but this is not always the case. For example, a parent may act as the *holder* of the verifiable credentials of a child (the *subject*)*,* or the owner can act as the *holder* of the verifiable credentials of a pet *(*the *subject* ).
- ***Verifier*** – a role that an entity performs by receiving one or more verifiable credentials, possibly included in a verifiable presentation, for the purposes of processing. Examples include employers, security administrators and websites.

In an equal interaction, people or organisations can alternate between different roles. So one example might be of a foreign national looking round an education fair and seeing a study programme they are interested in.

[12] https://www.w3.org/TR/vc-data-model/

[13] It should be emphasised once again that the same entity can switch between different roles.

This person wants to be sure and verify that the study programme is properly accredited. They are then acting in the role of verifier. In this case, the education institution has the role of holder and can show a verifiable credential to prove that the study programme is in fact accredited. When enrolling for the study programme, the same person is then the holder and the institution acts as the verifier, for example to check the applicant's prior qualifications. The person has a verifiable credential showing their prior qualifications and is able to provide it to the institution. Following successful enrolment, the institution can then issue a credential in their role as issuer, which the student can use in other interactions to demonstrate that they are enrolled at the institution.

### Roles in education

As described in the use cases, various scenarios are possible for education. For example, verifiable credentials can play a role in granting access to education or education facilities, access to the labour market, or demonstrating the quality of education. There are various organisations in the education sector that could be involved in issuing such credentials in the future, such as the Dutch education agency (DUO), the accreditation organization NVAO, Studielink, the Inspectorate of Education and the institutions themselves.

DUO is an obvious example of an issuer that can make statements about qualifications achieved based on the diploma registry populated by institutions. In the future, this could take the form of a verifiable credential. DUO also acts in another role as data verifier. For example, verifying whether someone actually holds the diploma for a party querying a diploma credential.
Not only that, there is also a need for the parties to maintain registries with verifiable (meta)data for use throughout the sector. This includes publishing schemas for diploma credentials and maintaining publicly verifiable information about accredited institutions and study programmes. It is explicitly not about shared registries on which personal or company data is held.

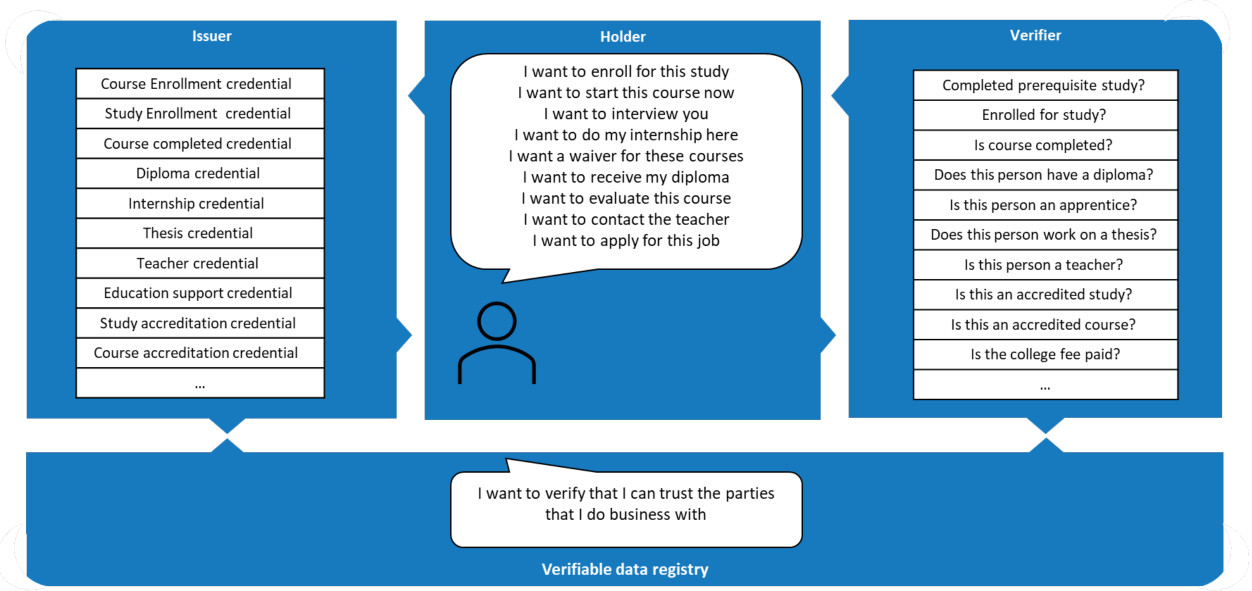

Issuer
Course Enrollment credential
Study Enrollment credential
Course completed credential
Diploma credential
Internship credential
Thesis credential
Teacher credential
Education support credential
Study accreditation credential
Course accreditation credential
...
Holder
I want to enroll for this study
I want to start this course now
I want to interview you
I want to do my internship here
I want a waiver for these courses
I want to receive my diploma
I want to evaluate this course
I want to contact the teacher
I want to apply for this job
Verifier
Completed prerequisite study?
Enrolled for study?
Is course completed?
Does this person have a diploma?
Is this person an apprentice?
Does this person work on a thesis?
Is this person a teacher?
Is this an accredited study?
Is this an accredited course?
Is the college fee paid?
...
I want to verify that I can trust the parties that I do business with
Verifiable data registry

Figure 3: Credentials in education

### Roles in research

Verifiable credentials are required in the domain of research to enable a whole range of different actors, such as businesses and citizens, to access data, digital services and laboratories. This allows society to participate more widely and benefit from research. Credentials can also play an important role in assuring quality and trustworthiness. There are various organisations in the research sector that will play a role in the future in issuing such credentials, such as the Royal Academy of Arts and Sciences (KNAW), the Dutch Research Council (NWO) and the institutions themselves. Similarly, international credentials from parties such as funding providers, Orcid, open science and publishers will also have a role to play when it comes to research.

For example, a European or national funding provider could act as the issuer of a 'funded research' credential. Researchers could use this credential as a 'quality mark' on the research website to show citizens who is funding the research. The funding provider may also act in the role of verifier. Researchers need to submit a lot of information when applying for funding, such as articles they have published or awards they have received in the past. In the desired situation, these could be provided by means of verifiable credentials. The funding provider would then be a verifier of these credentials.

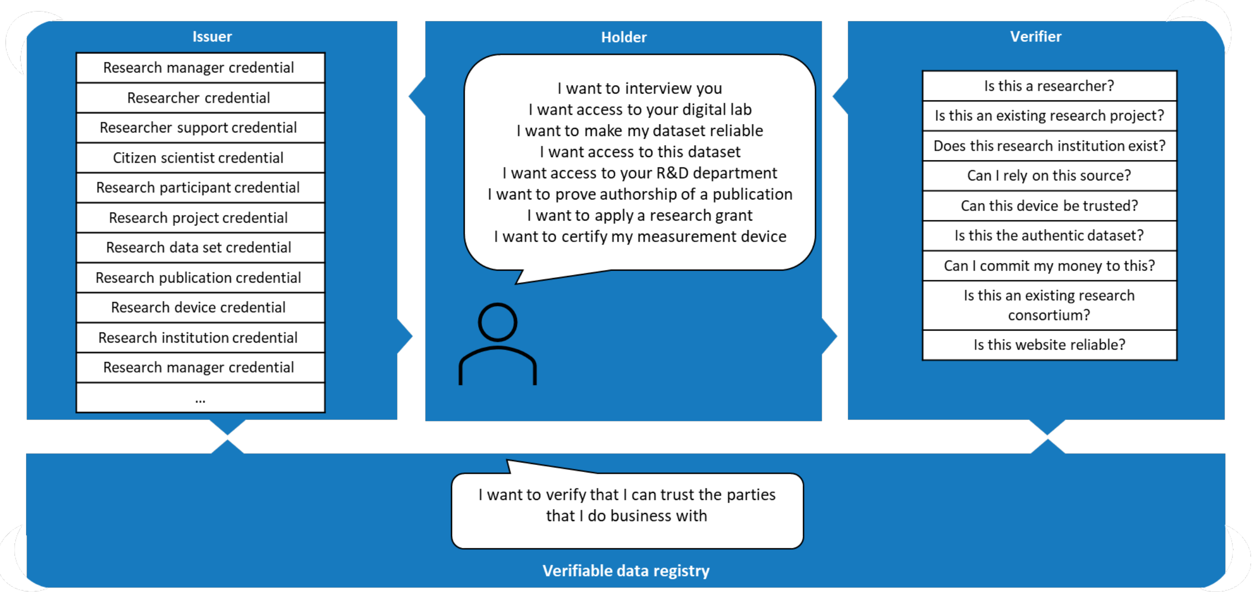

Issuer
Research manager credential
Researcher credential
Researcher support credential
Citizen scientist credential
Research participant credential
Research project credential
Research data set credential
Research publication credential
Research device credential
Research institution credential
Research manager credential
...
Holder
I want to interview you
I want access to your digital lab
I want to make my dataset reliable
I want access to this dataset
I want access to your R&D department
I want to prove authorship of a publication
I want to apply a research grant
I want to certify my measurement device
Verifier
Is this a researcher?
Is this an existing research project?
Does this research institution exist?
Can I rely on this source?
Can this device be trusted?
Is this the authentic dataset?
Can I commit my money to this?
Is this an existing research consortium?
Is this website reliable?
I want to verify that I can trust the parties that I do business with
Verifiable data registry

Figure 4: Credentials in research

## 4.2 The trust model

The granting of access is based on trust. Because several parties play a role in the ecosystem, the parties must have confidence in one another. The trust model for verifiable credentials is based on recognised roles and looks like this in the W3C data model:

- The verifier trusts the issuer of a received credential. For the verifier to be able to determine this, it is expected that a credential:
  - Either contains proof that the issuer has created the credential (i.e. it is a verifiable credential)
  - Or it is transferred in such a way that it is clear that the issuer has issued the credential and it has not been tampered with during transfer or when stored. The degree of trust required depends on a risk assessment by the verifier.
- All entities have confidence that the verifiable data registry is tamper-proof and provides a true picture of which data is managed by which entities.
- The holder and the verifier have confidence that issuers will provide truthful credentials about a subject, and that the issuer will revoke credentials without delay when applicable.
- The holder relies on a repository to store credentials securely, to not release them to anyone other than the holder, and store them in a sound manner.

The data model for verifiable credentials differs in a number of respects from the trust models where identities are issued centrally. The first difference is that the issuer and the verifier do not need to have confidence in the holder's repository, because it is clear from the credential itself that it is incontrovertible. Nor does the issuer need to know or trust the verifier. The trust model decouples the roles of identity provider and verifier, which often coincide in first and second generation IAM solutions. It introduces a flexible and dynamic model that reduces dependence on central entities and gives the user more choice.

## 4.3 Key concepts of the data model

In addition to roles and how they interact, the specification is based on a number of key concepts.

***Claims*** – A *claim* is a statement about a *subject*. A *subject* is a thing about which claims are made. Claims are expressed as a relationship between a subject, property and value. In the data model, a strong and diverse set of claims can be built up. These could be separate claims or several claims that relate to one another in the form of a *graph*[11].

***Credentials*** – A credential is a set of one or several *claims* made by the same entity. Credentials may also contain an identifier, as well as metadata that describes the properties of the credential, such as the *issuer,* the expiry date, a public key for the purposes of verification, the revocation mechanism, etc. The metadata can be signed by the *issuer.* A *verifiable* credential is a set of claims that are tamper-proof, linked to metadata and cryptographic proof regarding the *issuer,* such as a digital signature.

***Presentations*** – The promotion of privacy is one of the key assumptions underpinning this specification. Consequently, it is important that entities are able to be selective when providing information about their persona, so that only the information needed in the specific situation is disclosed. An entity can use different personas depending on the circumstances, so there could be a distinction between the person's professional persona, online gaming persona, family persona, incognito persona, etc.

***Verifiable presentations*** – present data from one or more verifiable credentials such that the origin (*authorship*) of the data can be verified. Verifiable presentations may be exactly the same as verifiable credentials in all respects, but can also contain data derived from credentials in a way that is cryptographically verifiable. In the latter case, the verifiable credentials themselves are not part of the verifiable presentation.

## 4.4 A conceptual description of IAM

Conceptually, there are two inter-related processes: one at the organisation level and one at the system level. At the organisation level, there are two parties who want to enter into a mutual relationship, for example to enrol on a study programme or to join the organisation as an employee. In this first instance, this involves establishing at the organisation level whether or not the two parties meet the requirements and expectations to enter into this relationship. During enrolment/onboarding, identifying criteria (e.g. name and date of birth) and qualifying attributes (e.g. prior qualifications),possibly along with other criteria set out in the organisation's rules, are used to evaluate whether the admission requirements have been met. The outcome is a decision to admit/employ (or otherwise) the subject as a student or employee.

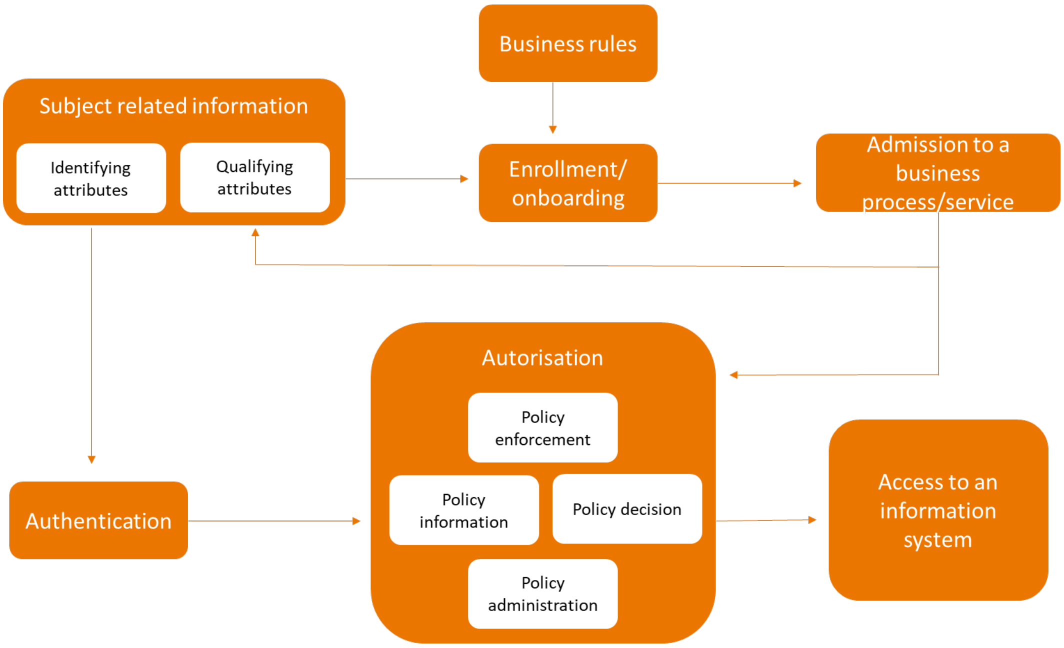


Figure 5: Functionalities and processes for IAM

Admission/employment of the subject results in the issuing of means of authentication to the subject and the granting of rights (authorisations) to enable the subject to access the information systems they need. From then on, the process of actually authorising and accessing the information systems is very similar to the familiar authorisation process, with new policies being defined and maintained and added to existing access systems. Because these policies need to operate in the same way across many different systems and organisations, agreements and standards are required to this end.

The introduction of verifiable credentials leads to changes at the conceptual system level, but not to the same extent everywhere in the system. Clearly, the biggest change is the way subject-related information is handled and is closely linked to authentication of the subject. Subject-related information is documented in a different way (i.e. in verifiable credentials or presentations), the information is provided by another role in the ecosystem (by the holder) and has different time behaviour (supplied on an ad hoc basis rather than in a predetermined way). Potentially, a number of steps in the process could be simplified or made more flexible, particularly if they are based on checking physical credentials or complex central administration systems for roles and rights. This can only work if clear agreements can be made (as a minimum) within the higher education sector about the role played by institutions and partners.

At the same time, consideration must also be given to the fact that other ways of interacting and sharing information – where the identification and qualification of the subject is not based on verifiable credentials – are likely to be around for a long time (and perhaps always will be).

## 4.5 Verifiable credentials in a business process

Verifiable credentials could lead to a higher degree of automation. The advantage for end users is that there is no need to create a separate account. Requests for proof can be dealt with directly from the wallet using verifiable credentials if the user gives their consent for this. In their role as verifier, the service provider can check the proof shown directly via the verifiable data registry without the issuer being informed of such.

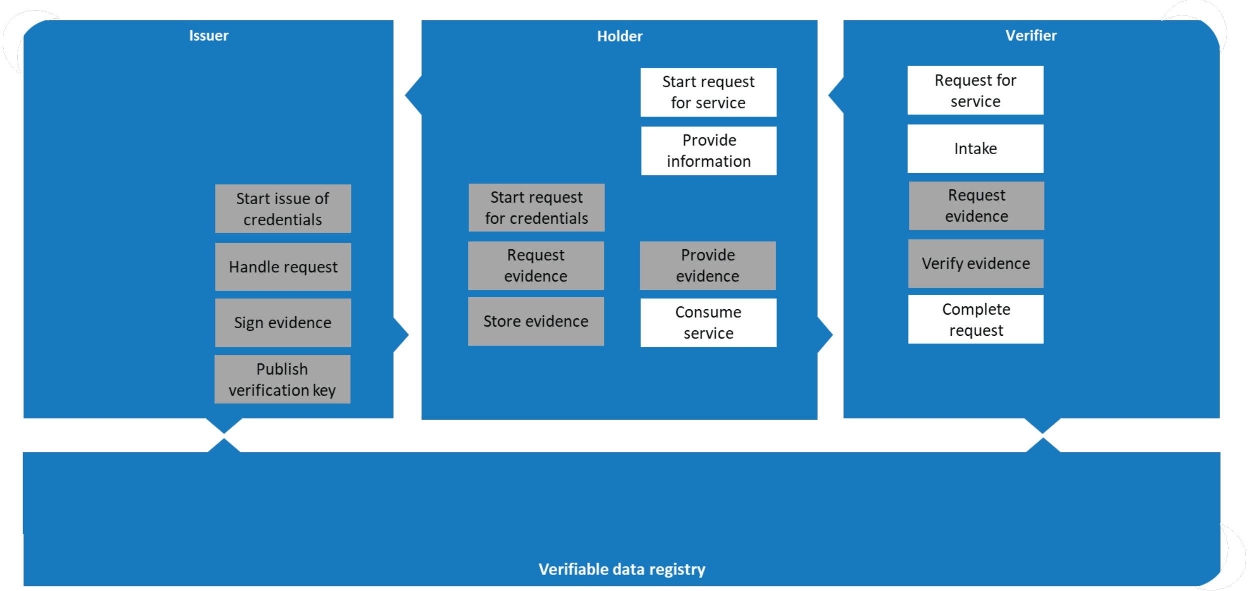


Figure 6: Application of credentials in a business process

# 5 Application architecture

The next section provides an outline of the application architecture. By using the same model for the application architecture as a foundation, HOSA provides an overview and creates a common starting point for discussions between the many stakeholders.[14] The application architecture also acts as a foundation for presenting various initiatives in a consistent way. The application architecture has been set up in such a way that initiatives from second and third generation IAM can be presented in conjunction with one another. This will allow SSI and more conventional forms of IAM to coexist in the future landscape.

In the application model for IAM, HOSA makes a distinction between society and its own sector. As stated earlier, HOSA expects Self Sovereign Identity to become more widely used in society in the future, and the sector should actively facilitate this in the interest of public values. This would offer benefits in terms of privacy, for example. However, if the sector is to encourage these developments, it also needs to make its own digital services and systems ready for this new future. Persons (and things) can use credentials issued outside the sector to submit a request to access systems and services within the higher education sector. The expectation is not that everything will be SSI, but that it will co-exist with conventional systems for logging in.

However, society does not end at the borders of our country and it moreover encompasses multiple sectors. So, under the heading of society, HOSA is also involved in public bodies, other sectors and other countries. These countries, sectors and public bodies use their own systems with their own rules and technical facilities. It is important for the higher education sector to be able to tap into these networks. As a result, all sorts of application functions that could address this have been included in the application model at the interface between the higher education sector and society.

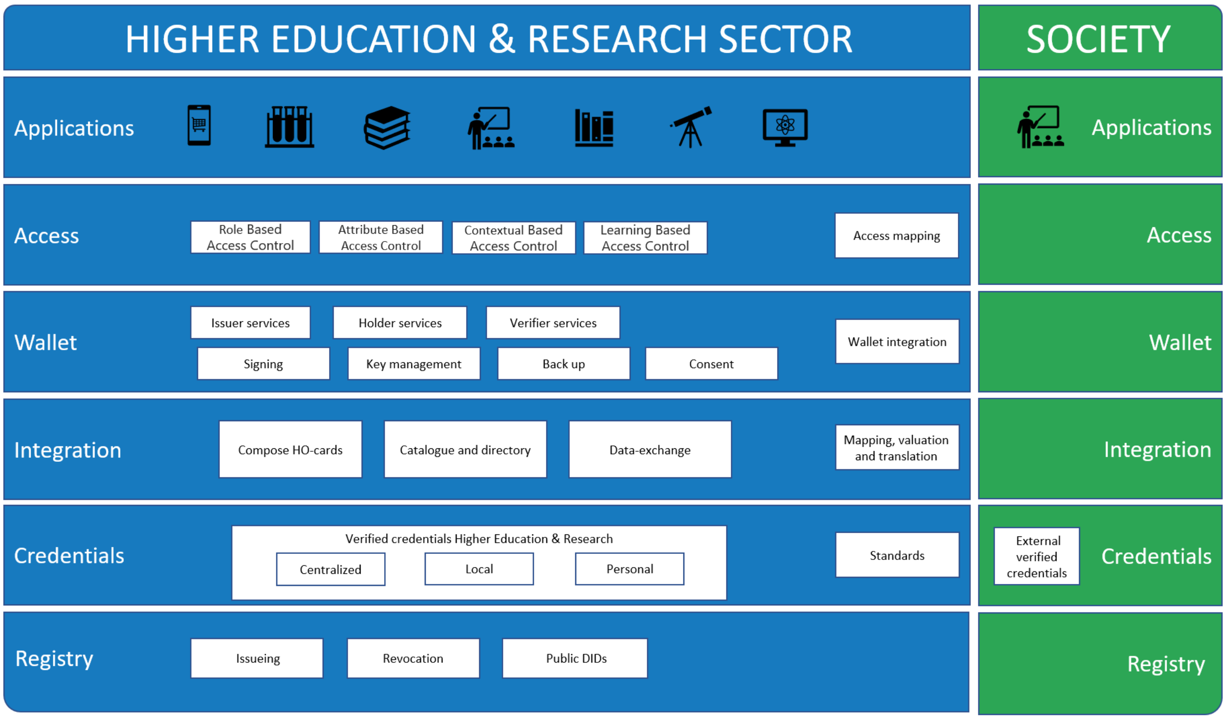


Figure 7: A layered application architecture for IAM

A number of information systems are required within the higher education sector in order to fulfil the proposed objectives. In the model for the application architecture, HOSA provides a structure that can be used to create an overview of the required information systems that work in conjunction with one another to meet

[14] This should preferably be linked to internationally accepted reference models. There appear to be very few of these at present. The Trust-over-IP model (ToIP, trustoverip.org) is the closest thing at the moment.

the intended objective of providing access. The model is future-facing and anticipates the trend towards Self Sovereign Identities (SSI). Current information systems from the IAM domain can also be plotted on the model. For this purpose, the model makes a distinction between six segments: Applications, Access, Wallet, Integration, Credentials, and Registries.
Each segment contains a number of functions that need to be able to stand on their own and to communicate with other functions and layers via well-defined interfaces. This has consequences for how the architecture is developed: solutions should not mix the elements, and agreements/standards need to exist for communication between the elements.

The section below explains what HOSA understands by this for each segment.

## 5.1 Applications

The Applications segment contains information systems that provide a range of different digital services to which end users need access. A number of examples are mentioned in the use cases, such as enrolling for a course in education, logging into a learning environment, using electronic measuring instruments or granting access to a laboratory. These services can be provided by institutions and sector partners. An important characteristic of sector services in the future will be that they often have a role within marketplaces or business platforms. Many different providers and customers come together here to benefit from a wide range of services. Institutions provide services to students, lecturers, researchers at other institutions, people who work in business, those who enjoy science as a hobby, and others. This creates major challenges when it comes to providing access to these services. Who is permitted to access a service and under what conditions? What proof does this person need to show?

The owner of an Application is responsible for indicating the trust level required to access it. To achieve this trust level, the end user will need to show verifiable credentials. A key principle here is that applications should request the minimum of privacy-sensitive data from end users, and no more than that required to grant access. Applications do this by facilitating the use of Zero Knowledge Proof. With Zero Knowledge Proof, you would only ask whether someone is over 18 years of age to be able to grant access, for example. Zero Knowledge Proof only requires a yes or no answer. No details of the person's age are made known. This prevents privacy-sensitive data from being unnecessarily disclosed to a verifier.

In addition, formal documents will also be 'credentialised' in this services segment. This means that formal documents are accrued in a structured way and made available on the basis of verifiable credentials. One example of this would be a diploma in which microcredentials from individual course modules can be verified with the issuer. This trend can be seen, for example, in the W3C VC version of Open Badges.

Convenience and ease of understanding for the user are important considerations when implementing applications that use credentials. This is primarily defined in the HOSA main principle of 'Accessible to all'. This encompasses the careful and clear design of processes for giving consent and sharing credentials.

**Logging in without a password?**

Self Sovereign Identity largely does away with the concept of logging in with a user name and password. However, not everything will operate entirely through SSI in the higher education and research sector. Services that provide long-term access via an SSI method can be set up without using passwords. Decentralised identifiers (DIDs) and verifiable credentials are used in this case. The credentials shared in this process can be used reliably, and no user profile needs to be created within the downstream application. Following consent, the credentials are supplied when the service is used on activation of the session.

**Data protection and auto-filling of forms**

In the longer term, the processes in these digital services will be able to achieve a much higher degree of automation using verifiable credentials than is currently the case. Proof can be provided automatically from a wallet if the user has given permission for this. Digital forms can also be automatically populated with data, or the user can instruct the wallet agent to auto-fill the data at the next visit with attention to data protection.

### Verifiable reviews

A major problem with current online services worldwide is that reviews of these services are not trustworthy. Users do not have the ability to check whether the authors of a review have actually purchased the service themselves. There is also a risk of someone posting numerous fake reviews in return for payment. The verifiable credentials system allows services to operate with verifiable reviews. Validated reviews can be posted without compromising privacy. In the domain architectures for Flexible Education and Research Data Management, reviews also play a role in respect of business platforms where functionality is provided to enable customers to post reviews.

### Granting and revoking consent

Under the GDPR, the consent of the end user[15] must be granted for the processing of data in certain cases. In SURFconext and eduID, it is already clear in the current situation which consents the end user has granted to service providers. Depending on the policy of the institution, an institution administrator can choose from three options for each service: an information screen, a consent screen, or no screen. Under the concept of Self Sovereign Identity, a user consents to the processing of certain data in the form of credentials. The user will then have an overview of all areas for which consent has been given and can also revoke consent. Support for revoking consent is not well automated within SSI as yet[16]. Nor is it easy for downstream systems to verify the status of a granted consent in the present situation. In order to create a reliable credentials-based SSI system, it is therefore necessary to check the status of consents for downstream systems via the wallet agents. Moreover, an agreement framework will need to be in place to ensure services comply with this requirement.

### Providing the minimum of data at the right time

Verifiable credentials make it possible to provide only the proof required to enable a particular decision to be made. Decisions around access would be taken on the basis of the verifier's access policy. Decision-making rules would be made public in advance so that people will not share the relevant data until they are likely to get a positive outcome. In addition, verifiable credentials enable real-time and up-to-date validation of the proof.

### Financial transactions

The concept of SSI facilitates scenarios in which financial transactions take place, including making payments. Here too trust is critical and research is being done into how SSI could be used in the financial world. Financial transactions are also relevant for HOSA in relation to business platforms in the domain architectures for Education and Research. This concept could potentially present a solution here in the longer term.

### Persistent connection

If SSI is used for defined services, a persistent connection will come into being for the parties concerned. This relationship between two parties will remain in place until one of the parties decides to sever the connection. These persistent connections are made possible through the use of DIDs. There is therefore no longer any dependence on a third party to act as an intermediary.

### Relevant developments

- Concepts and technical implementations of zero knowledge proof
- Large-scale pilots, e.g. for driving licences, access to government information and opening a bank account[17]
- Linking standards for OpenBadges to those for verifiable credentials. Open badges have been developed as an application for sharing information about educational achievements, but to date

[15] The EU General Data Protection Regulation.

[16] The legal and organisational implications of granting or revoking consent are also not entirely clear. It may be sufficient within the context of the IAM domain architecture for the architecture to facilitate a technically sound consent, but not get involved in the implications of this specific consent for the overarching business process.

[17] https://www.digital-identity-wallet.eu/

have not been issued as a verifiable credential. The educational standardisation organisation 1EdTech is partnering with W3C to bring this about.

## 5.2 Access

The Access segment holds the information systems used to organise access to the applications. Policies are used to determine whether a person or device is permitted to access the application. A new policy variant will be added for Access, but the principle of how access is granted will not change in any significant way. This is because decisions on access still need to be made in the same way: as in the current implementations, proof must first be collected or provided before a decision is made[18]. The credentials that have to be supplied for this would come from a wallet in the third segment as much as possible. In the current situation, the granting of access often takes place on the basis of roles. This is also known as RBAC and avoids the need to manually assign roles and rights to large groups. Familiar roles include the role of student and the role of employee.

More sophisticated components to grant the right of access operate on the basis of attributes or policies (access-based control (ABC) and policy-based control (PBAC)). This is already being applied in the current situation in relation to attributes and policies based on trusted internal source systems. However, in the present situation many current application landscapes still struggle to adapt their internal authorisation model to proof provided from external sources. Context-dependent attributes can be added in the future, such as an extra credential when a service is requested outside office hours (Context-Based Access Control). The user can provide this credential from the wallet.

In the longer term, there is the potential to consider more AI-based solutions. The system could then move to Learning Based Access Control (LBAC) where a change can be made in the request for required credentials based on pattern recognition. For example, if a large number of international students from Australia want to use a specific measuring instrument here in the Netherlands, it may be because a lecturer from a particular university has included this in their learning resources. LBAC can then be taught that the common factor of these students is that they are from this specific university and that the time in their time zone falls within office hours.

**Examples in the current situation**

If we look at the situation effective in 2022 in relation to the second generation of systems for IAM, we can already see moves towards the functions we would expect from third generation IAM systems. For example, the options to specify authorisation rules that grant access to an application. These authorisation rules can be based on data from a trusted source. This also plays an important role In HOSA's vision for the future, where it will also be possible to use SSI identities and credentials as a source to grant access to a second generation IAM service. The application can then rely on OIDC from SURFconext (or another service) that holds credentials supplied from the end user's wallet through third generation IAM.

Conversely, the SURF Research Access Management (SRAM) service can be seen as a link between 2nd generation IAM identities that want to use a service that is accessed via 3rd generation IAM. The credentials required for access can then be built up on the basis of data collected via SRAM and supplied to the relevant service in accordance with the standards that apply for data sharing in SSI and DID.

**Relevant developments**

- The Finnish IT Center for Science has developed a proof of concept for using SSI to manage access to privacy-sensitive human genomic datasets. The proof of concept is based on the ELIXIR Authentication and Authorization Infrastructure (AAI) and a commercial wallet.

[18] Note that the sequence will be different: in conventional systems, you start with an authentication, which produces an identifying number or role, and the appropriate attributes for authorisation are searched for in an internal system. In an entirely decentralised system, there is a set of attributes from which the identity and role can be derived by the verifier.

## 5.3 Wallet

The term wallet is often used in reference to Self Sovereign Identity. Wallets are applications for use by end users whose purpose is to store personal data in a protected, secure and personal way and to enable the user to present data to verifiers from the wallet. The wallet is directly comparable with a physical wallet used in real life. For example, end users can keep cards in their wallet that they can use as personal ID and currency to pay for things. In the context of Identities and Access, the wallet is a mechanism for storing combinations of public and private keys. It contains functionality that can be used to authenticate the user by means of credentials and also acts as a more secure version of a password manager. In addition, the user can sign reports from the wallet.

HOSA positions the functionality that allows users to work with credentials in the third segment in the application model. This includes creating, receiving, storing and signing credentials. As is apparent from the use cases, people or representatives of organisations often operate in several roles: holder, verifier and issuer. This means that the supporting functionality for this must be available in one and the same environment.

In the examples, wallets often run on or are accessed via a smartphone. Wallets can also run on or be accessed via laptops, desktops and other devices. In addition to wallets that function as an app, wallets that work as a web page in a browser are also available. Given the diversity of use cases, it is important that functionality for wallets should be offered both via an app and a browser. This will permit an any-device policy to improve accessibility and inclusivity.

**Personal wallet**
A distinction can be made in the higher education sector between different target groups based on their involvement in the sector. Employees of an institution, such as lecturers and researchers, but also students, are closely and directly involved in various processes that demand access with a high level of assurance. It is important for the sector to clearly define the requirements imposed on wallets by means of agreements and standards. In this way, the sector can align with standards from the public sector and the EU.

**Company wallet**
Institutions, sector partners and other parties also need the functionality of wallets. Organisations need to be able to demonstrate that they are trustworthy on the basis of credentials. In this way, people can be sure they are dealing with a real institution, a real research study or an accredited study programme. This will help to prevent fraud in the future. Institutions and sector partners can utilise the functionality of company wallets for this purpose. Integration with supporting information systems is important for company wallets in order to process large numbers of requests. Company wallets require additional features over and above those of personal wallets. Examples here could be extensive options for granting and instantly revoking roles, rights and permissions via delegation, a scalable underlying infrastructure to handle numerous simultaneous requests, and additional security measures. It is likely that different types of company wallets will come to be used within organisations depending on the area of business. For example, a finance department might require its own specific functionality.

**Wallets for custodians?**
A concept like Self Sovereign Identity also allows for animals, plants or things made by people to be given an identity. To this end, some people may acquire a third possible type of wallet that provides functionality to manage specific credentials on behalf of something or someone else. This is also referred to as a custodian wallet. This functionality could be considered in order to provide functionality to parents of students who are minors, for example. However, the current developments are moving more towards a preferred solution using credentials rather than an additional specific wallet. The holder would then be 'authorised' to act on behalf of another identity via a credential.

### Global functionality

In the desired situation, individuals and organisations will frequently have both the role of holder and verifier, but not at the same time for the same credential. The use cases include examples with a person who wants to know whether a study programme is actually accredited. In this case, the organisation will be in the role of holder of this verifiable credential and the individual is in the role of verifier. This means that wallets for individuals and organisations need to have functionality for both roles. The role of issuer will also crop up on a regular basis alongside the role of holder and verifier.

It is necessary within the higher education sector to agree on the substance of requirements for credentials for education, the rules for issue and acceptance, and the functionality required in wallets to support this. This will require collaboration between issuers, verifiers and wallet providers in an 'assurance community'.

There is also a requirement for functionalities such as signing, key management and recovery services. As is the ability to add qualified digital signatures to assure the authenticity and integrity of data and documents. Cryptographic technology, such as PKI, is frequently used to enable this functionality. The ability to add a signature is also important for trust when sharing data digitally. The verifier will be able to check whether the signature in a credential is still valid. Various methods are possible to enable this.

Recovery services are required if a person loses their phone, say, or wants to transfer data to a new device or create backups from a redundancy perspective. A backup can be used to restore or transfer data. Questions around this functionality include: what data and metadata should you include in the backup? Where should you save it and who should be able to access it? Resetting or restoring from a backup is far from a trivial matter in a decentralised environment. It's equivalent to asking where you get private keys if the original keys are lost. It is anticipated that some of the required functionality will be supplied by the wallet providers. Alongside this, consideration must be given at the level of the assurance community to functionality allowing credentials to be reissued or uploaded. This would require the issuers to retain information on credentials about which claims are made for a long time.

### Holder

For the holder role, the wallet is the functionality that enables the holder to obtain, generate, store, manage, protect and use privacy-sensitive data. Examples of confidential data include personal relationships with other individuals and organisations, passwords, biographical information, personal contact information, verifiable credentials, and any copies of formal documents. One method for managing personal relationships is using a DID manager. Some wallets include functionality for generating zero-knowledge-proof credentials.

### Verifier

Functionality is required for the role of verifier to be able to validate the presented credentials. This requires checks, e.g. of the format and the signature. The holder presents the credentials for a particular purpose, such as access, that require the verifier to make a number of decisions. These decisions are taken on the basis of defined principles or policy frameworks. At one extreme, these decision trees can be defined in automated procedures. The benefit here is that numerous requests can be handled by the organisation at the same time. At the other extreme, various checks can be carried out manually through an ad hoc procedure. Both options require digital support in the desired situation.

The role of verifier will need to be subject to requirements relating to the handling of credentials and being able to sufficiently justify the request to receive certain credentials. Checks for these requirements in relation to a verifier will form part of the trust system within which the credentials to be shared are significant.

### Issuer

It will frequently be important for an issuer in the sector to be able to issue verifiable credentials in large volumes. There needs to be a system by which requests from holders for the creation of verifiable credentials can be processed online via an automated process. It may not be necessary to implement this process entirely in the wallet itself. For example, the process could be initiated on the issuer's website. The holder would start the process of requesting a verifiable credential on the website. In processing the request, the issuer must be able to sign the credentials and transmit them to the holder. It must also be possible to publish the verification key used by verifiers for checking.

### Wallet integration

There are additionally a number of target groups that are somewhat outside the scope of standard services provision, but who still have some involvement in education and research. Examples include knowledge workers, trial subjects, inactive lifelong learners, or scientists who have left the organisation but continue to have ties to it. These are plotted in the application model in the green part for society. In the desired situation, these target groups will have their own wallet in which they can manage credentials from the higher education sector alongside other credentials. These might include microcredentials or other diplomas they have obtained, for example. The sector will make use of a Wallet Integration Gateway to enable this integration.

This gateway will have functionality to present, issue and validate credentials as well as formal documents. This will take place without reference to wallets or even documentation. In addition to technical interoperability, the gateway will also provide support for integrity, origin and other guarantees. Technical interoperability means users are free to use any wallet of their choice provided it meets the standards of the gateway. This means the sector will not have to shoulder the full technical burden of accepting any and all wallets people present when interfacing with the sector.

### Examples in the current situation

The sector does have comparable functionality at this level in the current situation, one example being SURFconext Consent Services. In the current situation, a user can indicate which of their data may be shared with others. Another example is the use of SURFteams to define groups in which federated accounts can be brought together, wich is used by the SURFdashboard, for example. Institutions can indicate which employees have which roles in respect of SURF. For example, they can indicate who is permitted to order licences or who is responsible for network administration. These roles (such as 'network administrator') are used by other applications, such as the Network Dashboard, for RBAC: the user is then able to use only the specific functions in the application assigned to that role.

### Relevant developments

- European Identity Wallet: Large-scale pilots are being carried out by the EU and legislation is being drafted (as an extension to the eIDAS Regulation) to make a standardised wallet available to all EU citizens.
- eduMij: A cost/benefit analysis was done last year on the added value of eduMij, which was originally conceived as a personal environment from which students could share their credentials or certificates with employers or other relevant parties.
- Wallet integration gateway: TNO is working on a gateway to facilitate integration between wallets that goes by the name TNO EASSI. This gateway would take some of the pressure off wallet providers, such that they do not need to maintain integrations with all other wallets themselves.
- Solid project: Solid is a project run by Prof. Tim Berners-Lee and MIT. The idea here is that individuals become the owners of data themselves and that this data is also stored in their own environment, the PODS[19].
- HR Career Wallet: This use case is from the DBC(dutchblockchaincoalition.org). This is a coalition of government agencies and stakeholders from business that have partnered to develop a joint wallet.
- The Global Legal Entity Identifier Foundation (GLEIF) is working on a verifiable credential for the Legal Entity Identifier (LEI)[20].

## 5.4 Integration

### Credentials catalogue

In the desired situation, services in the top segment of the application model will use verifiable credentials to grant access. When setting up these services, there will be a question about which credentials a person should

[19] Solid (solidproject.org)

[20] https://www.gleif.org

present in order to then decide whether they should be given access. The sector makes a catalogue available to help here that shows credentials issued in the sector with a description, a recommended level of trust, and a contact person. For example: this research university awards diploma in this form with these attributes, and this is the basis on which we establish that this type of credential can be assigned. The credentials catalogue is defined in one or more assurance communities. These are likely to include parties from outside the sector.

### Higher education cards

A further functionality in this segment concerns the generation of higher education cards. As described in the use cases, the higher education card is made up of a number of verifiable credentials that are brought together on the card. It must be possible to collate the credentials for these cards as a service to users in the sector. The wallets would then have functionality to allow data from the higher education card to be processed.

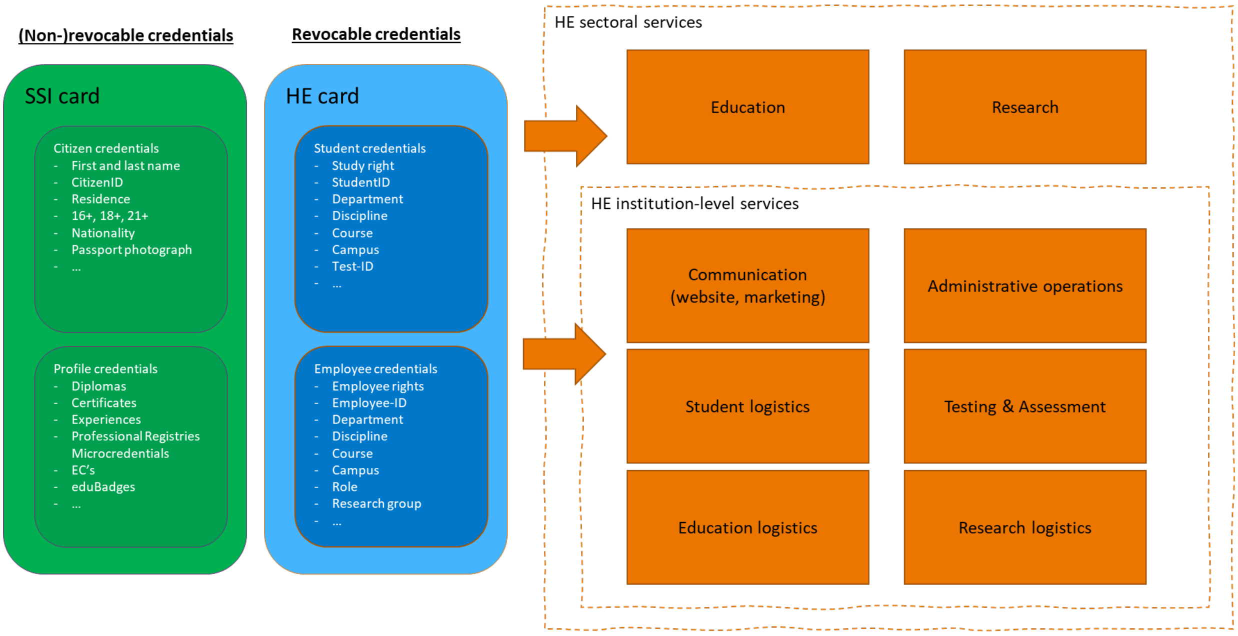


Figure 8: Positioning of the higher education card

### Data sharing

HOSA anticipates that a proportion of normal data sharing transactions that are distinct from IAM will be exchanged in the form of verifiable credentials in the future. Examples include student grades or numbers enrolled in courses. If a student is studying at two institutions, it must be possible to share this information. The student can consent to sharing this data via the wallet. Data can then be exchanged in the form of credentials in order to grant exemptions, for example.

### Mapping, translation and evaluation

Data sharing will take place not only within the sector but also more broadly in respect of society, including other sectors and countries. In other sectors and countries, terms often have different meanings and concepts may be structured differently, resulting in different content within data models. This will give rise to a need for mapping, translation and evaluation of other credentials. Here too, assurance communities can play a role.

### Examples in the current situation

In the case of student exchanges under the auspices of the Erasmus programme, terms have been standardised so that uniform terminology is used across the board. These standards can make it easier to determine the areas in which a student is eligible for an exchange. In HOSA's vision of the future, it should be possible to automate this by having an agency like Nuffic manage the mapping of different systems to one another. From there it would be possible to decide on the issuing of credentials based on values.

**Relevant developments**

- Current projects to develop a reliable system for sharing credentials include an initiative at Europass aimed at moving from paper-based certificates to verifiable credentials based on the European Digital Certification Infrastructure[21].

## 5.5 Credentials

**Format of verifiable credentials**

The W3C describes the format of verifiable credentials on the basis of four components. These are largely similar to the format of official documents, such as driving licences and passports. The four components referred to are as follows:

- Credential Identifier: this is a unique number on the basis of which the credential can be identified and looked up.
- Credential metadata: An example of this is the expiry date of the proof.
- Claims: each credential includes a number of claims about the subject to which the credential relates. For example, a passport may contain the claim that someone was born on 3 December 1981.
- Issuer Signature: the signature provides confirmation from the issuer of the credential that the credential has actually been issued. Verifiable credentials use a digital signature based on cryptography.

**Where to store and make available?**

For system as a whole to work, in the desired situation, verifiable credentials will be issued by the sector. These credentials will be generated using information systems that can be seen as source systems for these credentials. The reliability of the content of the credentials issued depends on the business process that adds data to the information system. This raises the question of which scenarios will be used to issue these credentials. There are mainly three options for education and research.

In the first option, the credentials would be stored and made available at national level by a sector partner. There would then be a single overview that could be queried for this credential. This would be a consideration if the data needs to be kept up-to-date at all times, such as in the case of financial credit transactions. So, to answer the question of whether someone still has sufficient credit to purchase a particular service.

The second option is for credentials to be held locally by the institutions. The data would not be located in a single national file, but could be retrieved in a decentralised fashion from institutions. This could be the case, for example, for a credential showing that someone is an employee at a certain institution. Clearly, privacy aspects are important here. The person may give consent from their own wallet, but the credentials will then be provided by the local institution.

The third option is for the credential to be held by the individual from whom it can be requested. In Tim Berners Lee's[22] vision, the user him or herself should be the owner of his or her own data. The idea here is that the information systems of organisations will then hold no or much less data about people. The data is then located with the person, or with a provider chosen and trusted by the user that functions as a kind of bank for managing data and credentials. This puts the user in a better position with regard to their information. By extension, credentials could also be held by and retrieved from the person. These credentials could then be supplied from another wallet as (sub)credentials when new credentials are to be issued within the higher education card.

[21] See https://europa.eu/europass/en/european-digital-credentials-learning-interoperability

[22] Solid (mit.edu)

**Examples in the current situation**

In the current situation, DUO provides the MijnDiploma's service ('My Diploma'). A diploma is issued once by an institution and remains valid for life. The fact that the diploma has been awarded is recorded in DUO. This allows people to request online digital proof of the diplomas they have been awarded. These are made available in PDF format, accompanied by a digital signature based on cryptography. The diplomas can only be requested directly by the individual personally and not by anyone else. However, it is possible to give digital permission to an employer, say, to retrieve a diploma on one occasion only. The PDF is a valid alternative to the original diploma and the individual can personally share it. In this case, the credentials could be used in a way similar to what we are accustomed to in the physical world.

**Relevant developments**

- Europass: Europass provides European Digital Credentials that are equivalent to paper certificates. Europass also employs a number of standards based on W3C, such as Digital Credentials for Learning[23].
- The data model for Verifiable Credentials[24]
- Microcredentials: pilots for microcredentials are being run by the UNL and the VH. The idea is that, in future, it will be possible to issue mini-diplomas for course modules. This is an example of verifiable credentials.
- OOAPI and the RIO data model provide a standard description of data to enable it to be exchanged. This model would need to be adapted to describe data in terms of credentials.

## 5.6 Registry

The concept of SSI has been widely applied in the world of blockchain. In true blockchain, data about the issuing of credentials is not held in a single place in a database; instead the data is distributed among several parties. This means that parties cannot modify data undetected. This is particularly important if mutual trust between the parties (or the users) is low. The applications also have a distributed set-up. This is completely different to how applications are set up in the current situation. For this reason, many experts argue against using blockchain for use cases unless there is a good reason to do so.

Not all use cases that occur require the use of blockchain. In many cases it is not necessary to work with a distributed append-only database (called a ledger in blockchain terminology – a term borrowed from the world of accounting). The following aspects need to be part of the considerations here:

- It must not be possible to modify data undetected
- There is a requirement for high availability of data
- There is a requirement to share data between multiple organisations
- There must be trust between organisations to ensure end users can get the service they need
- Shared agreements are required

HOSA has positioned the issuing and revocation of credentials in the bottom segment in the model, as well as the keys that can be used by the entities themselves to verify the relationships that may be established between entities. The content of the credential itself or privacy-sensitive data should never be located in this layer. These are purely keys that can serve as proof that particular credentials have in fact been issued.

Relationships between entities can be established by the entities themselves using decentralised identifiers (DID). One model for working with DIDs in a privacy-friendly way is not to store the DIDs themselves in a public registry, but only their hash. A verifier can then check whether the hash of the credentials presented to the

[23] European Digital Credentials for Learning | Interoperability | Europass

[24] Verifiable Credentials Data Model v1.1 (w3.org)

verfier is correct and the data is therefore valid. If someone invokes the right to be forgotten, for example, the relationship between the DID and the hash can be broken. The hash can then no longer be linked to the DID nor to the data that represents the DID.

Issuers must include their DID in a registry so that verifiers know which issuer they are dealing with. Issuers would use public DIDs for this. An issuer can additionally publish a schema of a credentials in a registry. The make-up of a credential would then be public and it would be clear which claims a credential from the issuer contains. A credential definition would also be made available in a registry. The credential definition contains the public DID, a schema and public keys.

Before an issuer can issue credentials, it is important to ensure there is a proper system in place to revoke credentials. Examples where this might apply include credentials that are only temporarily valid or revocation in the event of fraud or misuse. In the case of temporary validity, updates to the credentials and the registry would be carried out periodically. In the event of fraud, it must be possible to revoke credentials immediately. In the future situation, the revoking of credentials is likely to incur additional costs for public registries. Revoking credentials requires a revocation registry in which only the holder can see that a credential has been revoked. From a privacy viewpoint, there will also need to be a facility for the holder to generate proof of non-revocation.

**Examples in the current situation**

There are few examples in the current situation of initiatives that already operate on the basis of a registry where verifiers can check whether credentials have actually been issued. This is mainly to do with the maturity of the technology as described in the vision. SURF carried out a technical feasibility study into how ledger-based Self Sovereign Identity could work.

**Relevant developments**

- Sovrin: the Sovrin Foundation is a non-profit organisation that manages governance for the Sovrin Network. This is a public service that enables self-sovereign identity on the Internet.
- IDunion: the aim of the IDunion organisation is to create an open ecosystem for decentralised identity management, based on European values and regulations, that can be used globally.
- The European Blockchain Services Infrastructure (EBSI) facilitates public organisations in developing applications based on verifiable credentials. In time, private companies will also be able to join the infrastructure.
- Non-Fungible Tokens (NFTs). An NFC is a digital object owned by a user of the Internet. When you buy an NFC, you become the owner of the digital object. This is recorded in a blockchain by means of a unique token. NFCs can be bought and traded online.

# 6 Principles

The architecture for the higher education sector in terms of identity and access facilitates the various platforms, such as flexible learning. The principles[25] below are specific to the education domain and partly differentiate the principles defined at the general HOSA level for identity and access. We have guiding architecture principles for identity and access for the vision described, to act as a framework for setting up the desired architecture. They serve as a tool for and underpin configuration decisions.

## PRINCIPLE: USERS MANAGE THEIR OWN DECENTRALISED IDENTITY

Users manage their own decentralised identity (where 'decentralised identity' is defined in the foregoing description of the principle). You cannot 'control' your own identity – any more than your own partial identity (your self-image). Usually it is a matter of (just) being 'in control' of the data about yourself you have received from issuers and that you share with others. The 'control' then consists in being able to remove the data (by your own means) and deciding when to share it and with whom.

Completing online forms is often experienced by end users as unnecessarily time-consuming and irritating.[26] This problem could largely be done away with if services and facilities that currently still collect data using forms filled in by individuals (users) – that they then have to validate (sometimes manually) – could retrieve and validate the relevant data electronically. However, steps must be taken to ensure such services and facilities are not able to unintentionally retrieve personal data. This is not only not the intention, it is also prohibited by the General Data Protection Regulation (GDPR). The GDPR allows virtually any form of processing, including data sharing, providing the data subject (i.e. the person to whom the data relates) has voluntarily given his/her explicit consent for an arbitrary, but potentially specific purpose that the person can understand, i.e. that they want to do themselves, or want to have control over themselves. There are moreover other princilles in which consent is not always required.

### DESCRIPTION OF THE PRINCIPLE (WHAT IT IS)

What an organisation knows or believes it knows about a person is evident from the data registered about that person. Under Article 15 of the GDPR, this person has the right to be informed of data that is held about them. This principle additionally states that the person has the right to know this information or to have control over what happens to the data that has been collected.

### IMPLICATIONS AND CONSEQUENCES

The ability to have control of your data means that everyone can obtain attributes, at least those of which they themselves are the subject, by electronic means from organisations that issue them, and then present such attributes to other (often) digital services and facilities if requested by them. Ideally, no data should be shared between service providers without the knowledge or consent of the subject.

This means that anyone who wants to use services in the sector must have the means to store acquired attributes in a sufficiently secure manner, to present saved attributes to services and facilities upon request, and to manage the stored attributes and data sharing in a manner that is convenient for the individual.

[25] With thanks to Rieks Joosten, Senior Scientist at TNO

[26] National Ombudsman (2019). "Houd het simpel – Een onderzoek naar de gebruiksvriendelijkheid van digitale formulieren van de overheid ". Report no. 2019/046.

What a higher education institution or other sector partner can do with a person's data will in future be more tightly controlled by the person him or herself than is the case now. This is because the institution will only be able to use those elements of an identity that are necessary for the intended process.

## PRINCIPLE: USERS CAN RETAIN THEIR CREDENTIALS FOR AS LONG AS THEY NEED THEM

When creating credentials for diplomas, microcredentials or publications, for example, it is desirable to create a resource that can be used throughout the person's life. For certain credentials to be issued, the user must have the ability to obtain, store and use credentials that can remain available and be portable for life.

### DESCRIPTION OF THE PRINCIPLE (WHAT IT IS)

A user will have a wallet throughout their life in which attributes relating to that individual can be stored in a sufficiently secure manner, with functionality to allow them to present stored attributes to services and facilities upon request and to manage tasks in relation to the stored attributes and data sharing in a way that is convenient for the individual.

### IMPLICATIONS AND CONSEQUENCES

A wallet should ideally combine a storage function (i.e. acting as a safe) and an interface function. The storage function can be in the cloud, on a mobile phone, smart card, secure USB stick, etc. The interface function could be embedded in a browser or take the form of an app on a mobile device or similar. It can be 'customised' for different groups of users, and accommodate the needs of the group.

The wallet must be able to interface not only with the user, but also with services from other parties that act in the role of issuer or verifier. In the desired situation, the (electronic) protocols used for this will be standardised. We also foresee a need to be able to interface with additional new functions to do with revocation, the (legally valid) digital signing of data, documents, etc.

Standardisation is essential due to the large number of possible combinations of credential publishers, verifying parties and wallet suppliers. Regulation to this end is currently under development within the EU.

This principle means it is important that, if users can and want to replace the components that fulfil the storage and interface functions, issuers and verifiers must be able to effect this. It should also be possible to replace (parts of) the functionality. For example, if the user wants to use a different safe or wallet. This should not restrict availability of the functionality of the whole – the ability to receive, store and use credentials by parties that request it. A consequence is that the function must be retained if the wallet is replaced. The credentials must then continue to be available in the new wallet.

## PRINCIPLE: CREDENTIALS DO NOT CONTAIN MORE DATA THAN NECESSARY (DATA MINIMISATION)

Under Article 5(1)(c) GDPR, 'data minimisation' means that data (for processing – including retrieving or obtaining data) should be sufficient, relevant, and limited to what is necessary for the purposes for which it is processed. No matter how clear this might seem, there are different ways it can be viewed in practice.

One approach is to consider the request for data itself. So, if someone orders a book and is picking it up from a collection point, there is no need to ask for their name, address, telephone number, etc. All that is needed is for the collection point to be identified and (to be agreed) information to be supplied when collecting the book. This is down to the design of the (information) processes – in particular in the design of how information is requested, such as a form. This would involve making decisions about which data should be requested and which input boxes are 'mandatory' to enable the form to be sent or processed. This type of data minimisation should already be ingrained within every organisation (something that is not yet happening to a sufficient degree).

Another approach is to look at the form in which data is provided. Sometimes data is requested solely for the purpose of deriving other data: a date of birth could be requested to determine whether someone is older than 18, or a digital signature may be requested to determine that it was placed by a specific party. However, in these cases the requested data provides more information than is necessary for the actual purpose, and could also be used undesirably or unintentionally for other purposes. A comparable example in a social contest would be selecting job applicants based on their surname rather than their qualifications.

### DESCRIPTION OF THE PRINCIPLE (WHAT IT IS)

'Data minimisation' means that data processed for a particular purpose should be sufficient for that purpose, relevant, and limited to what is necessary for that purpose. This is primarily down to the design of (information) processes and the associated digital information request forms. It can also be about asking for information that is too specific for what is required.

### IMPLICATIONS AND CONSEQUENCES

The scope of digital forms and input fields should be limited to collecting the minimum information necessary. The parties are under a duty to comply with the GDPR and therefore apply this principle. Awareness needs to be raised among process and system designers to ensure they consider more alternatives when deciding on which information to request.

An important principle is that information systems should request as little privacy-sensitive data as possible from end users to enable access to be granted. They can do this by facilitating the use of a zero-knowledge proof approach. The use of cryptographic techniques such as zero-knowledge proofs (ZKPs) makes this possible.

## PRINCIPLE: TRUSTWORTHINESS IS ASSURED IN AN IDENTITY, AUTHENTICATION AND FEDERATION TRUST FRAMEWORK (LEVEL OF ASSURANCE)

If a person wishes to use a service or facility, the provider has to make a decision on whether to accept or reject their request. For that decision to be made, not only is information required but the data in question must be adequately validated. Such validation must be established before the decision mentioned above can be taken (because invalid data could lead to an invalid decision). Therefore, the party operating the service or facility needs to consider which criteria will form the basis for deciding that the data required to be able to decide on a request is valid for that purpose. Generally speaking, the criteria will depend on the risks the party thinks will arise if the decision were to prove invalid.

Data providers (issuers) can commit to requirements for determining and issuing this data, such as those specified by what are known as 'trust frameworks'. These trust frameworks not only define such requirements, but also establish sets of requirements ('levels'), each of which is increasingly difficulty to meet. This allows issuers to issue data at a certain level (according to a particular trust framework). The idea is that these levels make it easier for facilities and service providers to define their validity criteria. The sector aligns with and applies suitable frameworks through a clear selection process and criteria.

Furthermore, many trust frameworks (including eIDAS, NIST 800-63-B, ISO/IEC 29115) are restricted to data such as identifiers or name/address or similar attributes. However, these are primarily intended/appropriate to mitigate the risk a service provider incurs if it finds it necessary to serve a legal notice on an individual, or to be able to comply with legal duties.

### DESCRIPTION OF THE PRINCIPLE (WHAT IT IS)

In order to make a (run-time) decision on whether data can be processed in a valid way to produce a result (such as the decision to grant or refuse access to a service or facility), the party providing the service or facility must be able to define (design-time) criteria on the basis of which the (run-time) decision can be taken (electronically).

A trust framework provides for sets of requirements for different 'levels' (degrees of difficulty). Providers of datasets that meet the requirements for a certain level can label the data as such. For providers of services and facilities that may rely on this, it not only makes it easy to define validity criteria for that type of data, but also makes run-time verification easy.

### IMPLICATIONS AND CONSEQUENCES

In practice, it is evident that people often choose a framework because it is what others have chosen. Good framework choices contribute to ease of use. The sector aligns with and applies suitable frameworks through a clear selection process and criteria.

Trust frameworks facilitate the trustworthiness of data that must or can be shared between parties. They do this by specifying and labelling sets of requirements (such a label is referred to as a 'level'). Data providers can indicate which level their data meets. A party providing a service or facility that needs data from providers to enable such provision can use these levels as part of the criteria used to determine whether or not this data is valid for the provision of the service/facility. The use of a limited number of levels by a service/facility provider is much easier than the provider having to set up and manage complex validity criteria.

## PRINCIPLE: CAUTIOUS AND LOCALISED USE OF BIOMETRICS

The use of biometrics can greatly contribute to the accessibility and reliability of service delivery processes. Combining biometrics with a decentralised identity infrastructure, such as SSI, offers the potential for highly reliable identification and authentication processes that are attractive in technical terms.

This convenience and high reliability stand in contrast to the serious consequences for users in the event of leaks or misuse. Unlike an assigned identifier (e.g. a user name, student number or citizen service number), it is not easy to change a user's identifying biometric features. Biometric features cannot be separated from the person. Users may object to the use and documenting of biometric features. Moreover, biometrics are not equally reliable for all users (e.g. facial features can change – especially with young people), and biometrics provides new opportunities to breach security mechanisms (such as using a photograph or video instead of the person's actual face).

The processing of biometric data for the purpose of uniquely identifying a person is therefore prohibited in principle. In the normal course of things, users cannot be obliged to share their biometric data digitally. As a result, the number of instances where biometric data *can* be used (as a second factor) to increase certainty about a user's identity is very limited:

1. Explicit legal grounds, or
2. Strictly necessary and proportional for the intended authentication or security purposes,[27]or
3. Explicit *freely given* consent of the user

In most situations within higher education, the third possibility will apply. It is important that consent is freely given; this is not the case where there is a dependency relationship or a power relationship (such as employer-employee or institution-student/learner), because the person concerned will feel pressure to give their consent. Furthermore, there must be another alternative available, it must be possible for consent to be withdrawn, and refusal must not have any adverse consequences for the individual.

It is conceivable that future regulations could allow biometrics in specific cases (e.g. its use to achieve a certain high level of assurance), but even then it is essential to demonaterate that it is necessary and proportional.

### DESCRIPTION OF THE PRINCIPLE (WHAT IT IS)

Biometrics may only be used in exceptional cases, and its use is prohibited in all other cases. The tendency of the principle is to ensure that the right balance is struck and that solutions are considered that drastically limit the use of biometric data.

- *Biometrics* are used cautiously: their use is only possible if the conditions for exceptional cases are met. The universal use of biometrics is not permitted under law.
- *As a second factor:* access to systems and processes must not be based solely on biometrics.
- *Localised:* only in solutions for identification, authentication or security, in the direct use context of the user, under the direct control of the owner.
- *Alternative without biometrics should be the default:* accessibility for users who do not consent to biometrics must be assured.
- *Explicit freely given consent*: legal requirement, in any event for applications where no compelling interest is involved.

[27] Art. 9(2)(a) GDPR; Art. 9(2)(g) in conjunction with (4) GDPR in conjunction with Art. 29 GDPR.

This principle does not relate to the use of biometric data in, for example, scientific or medical research. Such use is outside the scope of IAM.

### IMPLICATIONS AND CONSEQUENCES

Enrolment/onboarding processes for access to education and research must avoid the direct use of biometric data. They could, however, use authentication services that apply biometrics, providing there is an explicit legal basis[28] for these servicesor for services with multiple methods where the user has freely consented to the use of biometrics. Such authentication services should only use biometric data for user authentication purposes, providing this data is not shared outside that context (in other words: biometric features can be used in direct, secure interaction with the user on their device, but are never shared beyond that session).

If biometrics are used, explicit consent must be given by the user for this purpose and a record of such consent must be kept. Viewing and revocation must be possible at any time. Users shall have the option of refusing use of their biometric data and have alternative ways to prove their identity.

Authentication processes in which biometrics may be used shall be designed such that no distribution or storage of biometric features takes place outside the session in which authentication is carried out. Biometrics used to enhance authentication may not result in the sharing of biometric data that is 'processed further on in the chain'.

Data minimisation, privacy-by-design and security-by-design are *essential* for this to happen, as are explicit accountability for and verifiability of biometric data use. Standards frameworks, standards, risk assessments and checks on the resulting measures are requisite elements. Some of these standards and frameworks are yet to be developed.

Using biometric data can create a strong dependence on market parties that supply (mobile) devices equipped with biometric sensors. When using biometrics, care must be taken to ensure that the technology deployed is sufficiently accessible on devices from multiple providers, that providers respect the standards and values of the education and research sector, and that implementations only process necessary biometric features, even if the device itself is able to release more data than is necessary.

The direct use of biometrics within education and research processes remains limited to cases for which an exception applies. Examples include situations where a high level of assurance about the identity of the user is required, such as for enrolment, assessments and examinations. A further example is access to and the sharing of highly confidential or privacy-sensitive data and processes, including an individual's own wallet, personal safes or other personal environments.

Derivative use is preferred when biometrics are used. The biometric features shall only be used in the authentication process, but not shared beyond it. The authentication process must not leave the environment over which the user has full control. For example, an individual's electronic identity document and biometric features included on it may have contributed to highly reliable authentication or a signature, but the biometric data itself may not be shared in the credential or claim issued.

[28] At the time of writing, such a legal basis does *not* exist!

# Annexes

# Annex A: Consulted persons and bodies

IAM Working Group

- Mark de Jong (Inholland)
- Caspar Terheggen (RU)
- Michiel Schok (SURF)
- Tom van Veen (SURF)
- Menno Scheers (VU)
- Mark van Bree (Saxion)
- Stefan Suurmeijer (RUG)
- Maarten van Schie (LU)
- Femke Morsch (SURF)
- Henk Schouten (HHS)
- Jan Over (EUR)
- Alexander Carlucci WUR
- Joël van der Elst (UL)

HOSA Steering Committee

- Jan-Willem Brock (Leiden University)
- Hans Louwhoff (SURF)
- Anton Opperman (EUR)
- Rose of Iperenburg (HAN)
- John Kropman (Fontys)
- René Schenk (Avans)

Sounding board & brainstorming group

- Sterre den Breeijen (TNO)
- Johann Schreurs (DUO)
- Jelle Nauta (DUO)
- Niels van Dijk (SURF)
- Menno Nonhebel (KNAW)
- Alexander van den Wall Bake (TNO)

Interviews

- Bob te Riele (RvIG)
- Andre de Kok (RvIG)
- Jimmy Snoek (Types)
- Christien Bok (SURF)
- Erwin Bomas (Kennisnet)
- Bart Cozijn (BZK)
- Caspar Terheggen (Radbout University)
- Joris Dirks (Studielink)
- Bart Jacobs (Professor of Security, Privacy and Identity; Radbout University)
- Frank Snels (Twente University)
- Stephan Okhuijsen (VU Amsterdam)
- Rieks Joosten, TNO
- Michiel Kraaij (WUR)
- Frank Niesten (Fontys)
- Nuffic/Erasmus+
- Andre Koot (Sonicbee)

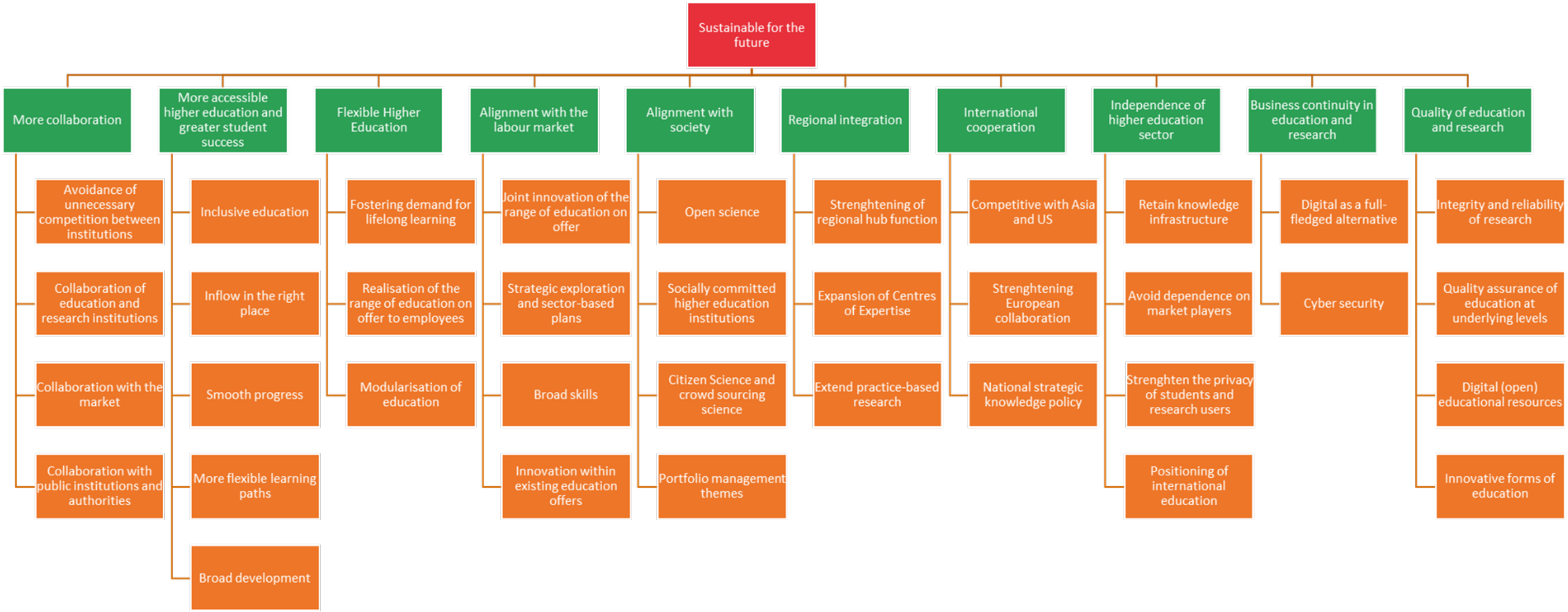
Review

1e. Sounding board & brainstorming group<br>
2e. SURF Enterprise Architecture<br>
3e. IAM Working Group<br>
4th. Higher education architectural council (ArchitectenBeraad HO)<br>
5e. Sector partners (Studielink, DUO, NWO, KNAW, TNO, MBOdigital, Kennisnet)

Sessions

- Edustandaard presentation
- Session with eduID Team
- EWUU
- CSC HBO
- TNO technical session on SSI
- Sector partners (Studielink, DUO, KNAW, TNO, MBOdigital, Kennisnet)

# Annex B: Higher education sector objectives structure



Sustainable for the future

More collaboration
- Avoidance of unnecessary competition between institutions
- Collaboration of education and research institutions
- Collaboration with the market
- Collaboration with public institutions and authorities

More accessible higher education and greater student success
- Inclusive education
- Inflow in the right place
- Smooth progress
- More flexible learning paths
- Broad development

Flexible Higher Education
- Fostering demand for lifelong learning
- Realisation of the range of education on offer to employees
- Modularisation of education

Alignment with the labour market
- Joint innovation of the range of education on offer
- Strategic exploration and sector-based plans
- Broad skills
- Innovation within existing education offers

Alignment with society
- Open science
- Socially committed higher education institutions
- Citizen Science and crowd sourcing science
- Portfolio management themes

Regional integration
- Strenghtening of regional hub function
- Expansion of Centres of Expertise
- Extend practice-based research

International cooperation
- Competitive with Asia and US
- Strenghtening European collaboration
- National strategic knowledge policy

Independence of higher education sector
- Retain knowledge infrastructure
- Avoid dependence on market players
- Strenghten the privacy of students and research users
- Positioning of international education

Business continuity in education and research
- Digital as a full-fledged alternative
- Cyber security

Quality of education and research
- Integrity and reliability of research
- Quality assurance of education at underlying levels
- Digital (open) educational resources
- Innovative forms of education

# Annex C: Sector aspirations

The higher education sector has high aspirations in the field of education and research. Many collaboration partnerships and discussions already exist that can move this forward, but these are as yet insufficient to shape the ambitions at the sector level. The Ministry of Education, Culture and Science has therefore worked with the sector to set a number of goals in the strategic agenda for higher education and research[29]. The emphasis here is on (regional, national and international) collaboration and the independence of the higher education sector. The following sections briefly discuss these ambitions.

### Regional and national collaboration

The strategic agenda states that greater regional and national collaboration needs to take place between the various institutions in higher education. To strengthen the pivotal role of higher education institutions regionally in boosting innovation and knowledge transfer, for example. The region benefits from a clear approach from the higher education sector. There should be not be any competition between institutions within the region in this respect. The higher education sector can play a binding role in projects in a region that transcend disciplines both in terms of content and facilitation of realisation. This would need to involve a more prominent role for practice-based research in order to make continuity in the region visible. A good model for this might be students from the region implementing this based on knowledge and skills from national higher education services that are offered by the sector for the collaboration and sharing of joint research and developments, for example. This can also be realised in lifelong learning by professionals within the region. An accessible digital identity and verified logical access control is a prerequisite for regional and national cross-sectoral collaboration with companies and public bodies. Such an identity transcends the boundaries of the individual organisations and also transcends the boundaries of the higher education sector.

### International collaboration

There is growing global competition in education and research. Countries like China, the United States, as well as neighbouring countries like Germany, are making rapid and ambitious investments in education and research. Many emerging economies are evolving from countries with low-cost labour to knowledge-based economies. Consequently, collaboration at the European level is becoming increasingly important; the changing geopolitical context also requires a more strategic knowledge policy. To remain competitive, national and international collaboration – particularly at a European level – is needed. Initiatives such as Erasmus Without Paper are already implementing this. The Netherlands has an excellent, open research system that scores highly in Europe and has partnerships with various European universities. The following Dutch universities participate: Eurotech (TU Eindhoven), Aurora (VU), CHARM-EU (UU) and YUFE (UM). Need to strengthen collaboration within the EU to remain internationally competitive with Asia and the US. Institutions are more likely to collaborate in international consortia. The use of a recognised reliable international digital identity and monitored logical access control is a prerequisite for international collaboration.

### Flexible higher education

Greater flexibility in higher education is necessary to make education better suited to the different characteristics and needs of the various target groups. A second reason is that digitalisation, globalisation and the ageing population are changing the labour market that higher education prepares for. These trends are affecting the type of work, the quality of work, and the required skills and competencies. The modularisation of study units and qualifications therefore needs to be supported, so that students can study in a flexible way in terms of pace of study, location, composition of subjects, depth of content and learning method.

With flexible higher education, the mobility of education participants increases sharply and the focus is on the individual participant in education instead of the institution. Digital identity is linked to the person and coordinated by the education participant.

[29] Source: Strategische agenda hoger onderwijs en onderzoek – Houdbaar voor de toekomst

### Lifelong learning

Ongoing changes in society and the type of jobs available, along with the skills they require, mean that developing knowledge and skills is a lifelong process. Lifelong learning aims to help citizens equip themselves for changing job roles throughout their lives. Innovative lifelong learning solutions are required to create a range of education offerings and the necessary resources to align this with the labour market. This means course content should closely reflect changes in the jobs market. Lifelong learning necessitates the holding and use of digital identities that are not only suitable for use across institutions, but also throughout the higher education sector.

### Integrity and reliability

Integrity and reliability are critical for there to be confidence in education and research in society. For example, in the case of education, employers need to be able to proceed on the basis that graduates have the appropriate level of knowledge and competencies. A variety of checks and balances in the process ensure this integrity and reliability. For example, an examinations board that signs that a student has met the requirements or an audit committee that approves the quality of education. In the future, these signatures are likely to be digitalised so that they can be used or shown again at a later time. This allows for efficiency to be created, but also greater confidence. Integrity and reliability also play an important role in research. It can be difficult for citizens to differentiate true scientific knowledge on the Internet from fake content. This problem will only increase in future. In order to enhance confidence in research in society, new digital tools are needed that, for example, organise the traceability of scientists or that can demonstrate that a particular website for a scientific research study is actually reliable.

### Independence

Institutions in the higher education sector provide education and conduct research in accordance with public values. For example, public values ensure that education is widely accessible to participants in education and that institutions within the higher education sector are independent of government and private market players. Public values in higher education are not only essential for the institutions individually, but also for Dutch society.  The public values that are fundamental to the higher education sector are coming under increasing pressure due to greater digitalisation of the higher education sector. The higher education sector is making use of cloud services from international commercial providers to an ever greater degree. As a result, the higher education sector is increasingly dependent on the roadmap of a limited group of commercial providers. The higher education sector wants to prevent the independence of education and research from coming under further pressure.

### Business continuity

The Cyber Threat Analysis for 2020–2021 [30] (published annually by SURF) outlines an increasing threat landscape, with the risk of cyber attacks growing to a crisis point. Such a crisis would not only be of great significance for the institution concerned, but would also have an impact on the entire sector. A number of organisations in the sector have been the victim of ransomware attacks that forced them to close for a few weeks and completely shut down operations. Business continuity was also threatened due to COVID. Institutions in the sector had to rapidly roll out fully online education and research in order to offer continuity of education and research. Assuring business continuity is of great importance for the sector services of the future where HOSA defines the frameworks.

[30] Source: CYBERDREIGINGSBEELD 2020-2021 • ONDERWIJS EN ONDERZOEK • SURF

# Annex D: Developments

This section describes developments in functionality and technology for the Identity and Access domain. A number of issues that may be relevant to future developments in the higher education sector have been identified. The developments considered as potentially relevant by the Identity & Access Management working group come from scientific publications, policy documents and the media.

## 1. Developments in the area of identity

**Dutch Digital Source Identity**

At the beginning of 2021, the Dutch government published a vision on digital identity and the associated infrastructure and sent a letter to the Dutch Parliament outlining this[31]. The letter describes the challenges and opportunities and outlines a future in which the Dutch government takes on or expands four areas of activity: (enabling) the sharing reliable data, organising access to digital services, issuing a recognised digital source identity, and drafting and enacting associated legislation and regulations around digital trust.

The digital source identity is the set of basic attributes held by the government on the basis of which identity documents (virtual and physical) and authentication means can be issued. The digital source identity is intended for use by citizens. They can share self-verified data with other parties as they see fit. To this end, the Dutch government is working on a single authoritative source: the digital source identity. This would be a digital version of the identity data of citizens registered by the Dutch government.

The Wettelijke identiteitsdocument (WID) [legal identity document] can be compared to a physical passport or identity document. Citizens will be able to use their WID to establish their identity at a bank to get a bank card, or to get an ID card from an organisation. Bank cards and organisation access cards are examples of 'derived' identity devices. The vision is that, in principle, parties in the public and private sector will be able to issue derived identity devices.

Citizens will be given access to their data by means of authorised identity devices. Therefore, they will not use the digital source identity, but rather derived identities in the form of an authorised identity device. This authorised identity device uses the digital source identity to base its trustworthiness on the 'authoritative source' of the Dutch government. An example of an identity device could be an app (wallet) on a mobile device where the user of the app can personally decide who to share available identity data with.

**Public sector eID**

Public eID schemes are normally provided by government agencies or legal entities with a legal function to give citizens a secure method of accessing online services. Enrolling with DUO and Studielink takes place using DigiD. Under current legislation, DigiD cannot be used as identification for private purposes.

**Private sector eID**

Social media companies in particular compete to offer identity solutions, but they are not the only ones. Social login is the name for identification and login solutions offered by social media companies. These solutions tend to score high in terms of ease of use and user experience, as users are typically able to create accounts with just a few clicks and reuse them for a range of other services. However, they score relatively low in terms of the level of trust and security they offer. These accounts typically do not have a proof of identity stage where users have to prove who they are with legal proof of identity and physical verification. As such, they are not suitable for more sensitive situations where it is essential to verify who the user actually is.

[31] https://zoek.officielebekendmakingen.nl/kst-26643-743.html

Just six big internet platforms dominate social login. They account for 87% of the social login market: Facebook, Google Sign-In, Instagram, LinkedIn, Twitter and Amazon. Facebook and Google are driving these developments, with 41% and 35% of European users respectively.

Financial institutions and banks also have a strong position in this market. They have developed strong identification solutions to enable customers to access their online banking platforms. In many cases, they have taken it a step further offering these identification solutions to other online services. Mobile network operators also offer their customers modified SIM cards that enable mobile identification solutions. Finally, a new set of dedicated digital identity companies and digital identity networks has emerged, which do not necessarily come from an existing user group but provide a secure and straightforward identification method.

**Bring Your Own Identity (eID)**

Bring Your Own Identity (BYOI) is a growing trend in the world of digital identification. It involves reusing a single digital identity to access a range of different online services from both the public and private sectors. EID schemes for the public sector, for example Chave Móvel Digital in Portugal or the German EID scheme, are a form of BYOI. However, an increasing number of private organisations are also offering BYOI solutions for their users.

The origin of 'Bring Your Own Identity' can be traced to the proliferation of digital services, each of which requires a different password to access. Many users are fed up with having to remember and manage so many passwords and identification procedures. In response, companies have developed a range of different identification options providing a secure, user-friendly way to prove who you are. These solutions can be used across all services, from retail to banking and entertainment.

A major drawback of the growth in BYOI is that it makes it easy for big web platforms and companies with large user files to couple a lot of information about users and so create extensive profiles. As far as the higher education sector is concerned, this is considered to be in conflict with public values. In addition, the use of 'Bring Your Own Identity' leads to dependence on an intermediary party. This intermediary party has a great deal of power over the relationships a person has with providers. If the intermediary is no longer available or denies access to the user, this person will lose all these relationships.

**Self-Sovereign Identities (SSI)**

Self-sovereign identity (SSI) is a movement around identities that gives the individual user full control over their own identity and data. The concept of SSI is becoming increasingly popular according to market analysts. A number of terms for SSI are used, with blockchain identity, decentralised identity and portable digital identity being among the most popular, although these terms are still somewhat limited as a description of SSI. For example, it is possible to have a decentralised identity schema in which the individual is not involved, or that does not give the individual control over their identity.

One crucial aspect of SSI is that it supports a change in the way identity is handled by companies, users and government agencies. In its purest form, SSI uses Distribute Ledger Technology (DLT), of which blockchain is the best known example. Blockchain is a common element in the architecture of SSI solutions. Blockchain provides an underlying 'trustworthy' basis for proving that shared identity details are correct and have not been falsified.

It can provide this basis because of its inherent strengths, such as the distributed ledger and its setup in line with the principles of privacy by design. By making a ledger of transactions accessible to multiple parties, data cannot be changed or falsified undetected. Privacy by design works by giving the user full control over what data they share and the ability for a party to verify credentials presented without the issuer of the credentials being made aware of this. It works in a similar way to a physical passport: the authorities are not aware you have presented your passport to hire a car, for example.

## 2. Developments in the area of access

### Out-of-band authentication (OOBA)

Out-of-band authentication (OOBA) is an authentication process that uses a communication channel that is separate from the primary communication channel, with two entities that attempt to establish an authenticated connection. Using a separate verification channel makes it much more difficult for an attacker to intercept and undermine the verification process (i.e. via a man-in-the-middle attack), as the attacker would have to compromise two communication channels for this. Examples of forms of OOB authentication include codes sent by text message to a mobile device, authentication via a voice channel, codes sent via push notifications to a mobile app, and codes sent to or received from a trusted execution environment connected to the host device trying to establish an authenticated connection.

Examples of where OOBA is used include SURFsecureID and online banking. In order to complete the login process, an authentication code is sent by text message to the account holder's mobile device. OOBA is used to log in using a second factor via another channel. The second factor prevents identity fraud, making it possible to assign a higher degree of trustworthiness to an identity on behalf of an institution, for example when processing figures or internship contracts. One disadvantage here is that a mobile device is often used for the second factor, but the same mobile device will in many cases also be used to access the functionality. Despite the fact that there are two channels, if all transactions take place on the same device, security is not necessarily enhanced.

### Continuous authentication

Continuous authentication is a way to give users access to online services based on acceptable risk levels or contextual information. Continuous authentication is passive, while traditional authentication is considered to be active. In all cases, the user has to specify an authentication factor (e.g. knowledge, ownership or biometrics) in order to gain access. Continuous authentication uses information, such as browser metadata, user location, passive life detection or time of day, to arrive at an authentication score. During an online session, the authentication score for granting or denying access coresponds to the service provider's risk models for that activity. For example, simply viewing account details can always be allowed as long as the risk score is within the trusted range, because the company considers the viewing of information (even by a fraudster) to be benign. A financial transaction during the session will result in the user being asked to actively provide an authentication factor for the payment authorisation. The technology underpinning continuous authentication is Artificial Intelligence that establishes identity based on a context. At present, CA is mostly used within organisations offering different online services from the same organisation, rather than a federated operating model such as SURFconext.

## 3. Developments in the area of Cloud identity services

In addition to traditional IAM solutions, pre-configured standardised cloud-based IDaaS services are being developed for or as part of SAAS with logical access management, single sign-on, user provisioning, digital identity, compliance and both multi-factor and adaptive authentication.

### Identity as a Service

IDaaS is a platform for managing identities and providing access from the cloud. Azure AD Services from Microsoft is a good example of IDaaS. It can be used not only for Microsoft applications but also for third party applications. Applications can then be located in the Private Cloud, Public Cloud, or in the organisation's data centre. Microsoft also calls this mix of identity and access for on-premise and cloud applications the Hybrid-ID concept. Other companies like Google, AWS, etc. all have similar IDaaS functionality available.

**SaaS with integrated ID**

Cloud application (SaaS) providers have integrated an IDaaS component as part of their business Cloud applications – SAP, Salesforce, etc. are examples here. Organisations that choose this option may become less flexible over time than if they had implemented an independent IDaaS solution not tied to a particular supplier – one that allows users to retain full control over their identity.

# Annex E: Standards and technology

Digital transformation has increased the need for robust identity, access and authorisation standards suitable for remote working, multi-cloud environments, IoT, APIs and DevOps. Authentication for access is a core component and is central to the security and management of modern organisations.

Authentication events need to provide context for the key identity questions: who is the user and/or what is the device, where are they authenticated, when are they authenticated, how are they authenticated, what attributes have we assigned, and how and why have we provided them? All authentication protocols must be able to answer these questions. Over many years, the industry has developed protocols that provide secure authentication beyond the standard user name and password.

**SAML**

Security Assertion Markup Language (SAML) is a standard for the secure sharing of users' authentication and authorisation data between different organisations. SAML makes it possible to securely access services from different organisations via the Internet without the need to provide your own login details for each service or to log in to each service separately. SAML is widely used, especially in corporate system landscapes, but is considered less suitable for mobile applications.

**OAuth 2.0**

When a user successfully authenticates him or herself on a web application with an OAuth 2.0 service, the OAuth 2.0 service issues a token for this user account such that trusting parties can accept authentication on their systems. OAuth has become popular as an authorisation protocol due to the spread of APIs that allow developers to create applications that are compatible with web-based platforms. It is increasingly found in enterprise web and desktop applications to give user accounts access to applications for a range of purposes.

**OIDC**

In addition to SAML2.0, which is already in wide use, OpenID Connect (OIDC) is another HTTP-based protocol similar to OAuth. OIDC uses OAuth to provide a robust authentication and authorisation package that allows user accounts to access applications. It can also enable single sign-on (SSO) for users to different web-based applications by means of an OpenID identity, allowing clients to verify an end user's identity based on authentication performed by an authorisation server or identity provider (IdP). The user can reuse a single identity given to a trusted OpenID identity provider and be the same user on multiple websites. Like OAuth, OpenID is used in many consumer applications. The recent opening up of bank customer information to third parties makes extensive use of OAuth and OpenID protocols.

**FIDO**

The FIDOTM Alliance (Fast Identity Online) is a non-profit organisation established in February 2013 to address the lack of interoperability between strong authentication devices, as well as the issues users experience in creating and remembering multiple user names and passwords. The FIDO Alliance has developed specifications that define an open, scalable, interoperable set of mechanisms that eliminate the dependence on passwords for the secure authentication of online service users (passwordless).

FIDO authentication standards for browsers, operating systems, web servers and personal devices allow websites and applications to give their users the ability to unlock cryptographic login credentials using straightforward built-in methods, such as fingerprint readers or cameras on their devices or easy-to-use FIDO security keys.

**SCIM**

System for Cross-domain Identity Management (SCIM) ensures that user identity information is in the right place across systems. This allows data that should no longer be in a system, for instance because a user no longer needs to be included in that system, to be deleted. Since  this process is automated, relatively little effort is required for data to be added or deleted as required. For example, SCIM is used to add or remove information about the identity of users in different places in the cloud. SCIM uses an Application Programming Interface (API) that allows a computer program to communicate with another program. This standard aims to reduce costs and complexity and to build on existing protocols. The goal of SCIM is to move users in, out, and between cloud services quickly, easily and cost-effectively.

### Decentralized IDentifier Specification (DID)

The Decentralized identifier specification[32] (DID-Core) describes the architecture, data model, methods and syntax for establishing and using decentralised identities, such that the owner (controller) of the identity can have control of their identity without reference to third parties. The standard does not define specific technical implementations. The specification builds on the Verifiable Credentials Data Model[33].

[32] Decentralized Identifiers (DIDs) v1.0 (w3.org)

[33] Verifiable Credentials Data Model v1.1 (w3.org)

# Annex F: Current situation

In order to get a picture of the current situation with regard to Identity and Access, an inventory has been drawn up of initiatives and services around Identity and Access. The inventory is not exhaustive, but it can be seen that there are already many initiatives on the ground.

The inventory shows that initiatives and services within the sector are not always linked up. In order to set out the current situation in the area of Identity and Access, this domain architecture is based on existing services and initiatives from various organisations and partnerships in the sector.

During the inventory phase of generating the domain architecture, an inventory was made of various initiatives and areas of focus around Identity and Access via interviews, reports and sessions. Section 4.1 briefly describes a number of initiatives in the area of Identity and Access within education and research, Section 4.2 considers sectors outside education and research, and Section 4.3 details the key points for attention that came to the fore.

## 1. Initiatives within Education and Research

There are a number of initiatives around Identity and Access for Education and Research that address some areas of existing issues. A number of well-known initiatives are described below, including their intended objectives. The initiatives included are concerned with promoting inter-institutional use of identities to provide controlled access.

### eduID

Education is becoming more digital and more flexible. Students want to shape their own path through education. This creates logistical and administrative challenges. To address this, SURF is working with eduID[34] institutions to develop a single unique identity that students can use at any education institution before, during and after their studies.
The objective of eduID is to provide an overarching digital student ID that is not dependent on any particular institution. eduID is much more than a student number. It is a facility that is linked to a person. This stands in contrast to the current system with student numbers that are linked to an institution. It is no longer the institution but the student him or herself who is in control of (personal) data, courses followed and grades achieved. In the eduID project, SURF is developing a single digital identity for students in the Netherlands. Through their eduID, students will be known to their own institution, but they can also use it to identify themselves at another institution or to give permission for data to be shared between institutions.

### ORCID

ORCID stands for Open Researcher and Contributor ID and is an (alpha-numeric) code used to uniquely identify authors of scientific works. ORCID is a free, unique, persistent identifier that can be used by individuals involved in research, scholarship and innovation activities. The purpose of this identifier is to connect all those involved in research, science and innovation. The identifier uniquely identifies the participant and links the participant to their contributions across disciplines, boundaries and time.

ORCID is backed by a non-profit organisation of which scientists, institutes and organisations can become members. It is a community-based organisation that provides three related services: the ORCID ID, an ORCID record linked to the ID, and a set of Application Programming Interfaces (APIs) that facilitates registration and information exchange with ORCID records.

[34] Source: Wat is eduID nu precies? | SURF.nl

### Higher education institutions

Many institutions have their own IAM infrastructure and have initiatives or projects ongoing in the area of IAM. In addition to IAM for digital identities and access for their own employees and students, they also wish to give controlled access to users from other institutions or 'guests' from outside the education sector. Other initiatives are looking at enabling login using additional tokens.

### SURF Research Access Management

Frequently, the work of researchers is not confined to their own institution, but will often be international in nature. The SURF Research Access Management[35] service from SURF supports the education sector to collaborate in organising and managing access to research services. This makes it easier for researchers to collaborate with colleagues within and outside their own institution. You log in with your institution account and manage access to services for your research collaboration yourself. The FIM4R initiative documented the identity and access challenges in a report. The AARC project (Authentication and Authorization for Research Collaborations) was set up in Europe in response, one of the results of which was a 'Blueprint architecture' (AARC BPA). SURF used this architecture in the 'Science Collaboration Zone' (SCZ) project that led to the development of the SURF Research Access Management.

### Edustandaard IAA working group

The Access[36] working group was initiated by the Standardisation council and its role is analysing how future visions on access in education sectors fit together, identifying issues that make it difficult for them to interface, and proposing an approach to ensure they can interface with one another. The target group for access is not limited to students at an institution, but also includes education professionals, researchers and employees. The IAA working group is made up of participants from primary education, general secondary education and vocational secondary education, higher professional education, academic higher education, SURF and the Ministry of Education, Culture and Science.

### European Student Identifier (ESI)

The European Student Identifier (ESI) [37]is a form of digital identification that students can use to uniquely identify themselves. The ESI was set up in the context of the Erasmus+ programme. In fact, it is only relevant within the programmes and services offered by Erasmus+ to participating institutions. This identification is required if they want to access online services required for student mobility in the context of Erasmus+. In the first instance, this is for registration in the administrative systems of the European education institutions concerned. In short, the ESI supports and facilitates international student mobility and transnational collaboration between higher education institutions within Europe. A central ESI hub will be available within Europe based on the European Student Identifier to enable access to Erasmus+ services; this hub is known as the 'MyAcademicID Proxy'. MyAcademicID builds on the eduGAIN, eIDAS, European Student Card (ESC) and European Student Card Number (ESCN) schemes.

### Diplomas and Credentials European Blockchain Partnership

DGDIGIT (EU) has piloted the use case of diplomas over recent years. This is a European initiative, introduced by the Netherlands (DUO) and facilitated by DUO (User Group Diplomas and Credentials European Blockchain Partnership). A large number of member states participated in this initiative and have come up with a number of use cases for the field of education in relation to digital identity.

[35] Source: https://www.surf.nl/surf-research-access-management-veilig-en-eenvoudig-toegang-tot-onderzoeksdiensten/wat-is-surf

[36] Source: https://www.edustandaard.nl/oprichting-werkgroep-iaa-inventarisatie )

[37] Source: https://wiki.geant.org/display/SM/European+Student+Identifier

## 2. Initiatives outside Education and Research

A large number of identity initiatives are taking place outside the sector. The most important of these are listed here[38].

### European – eIDAS and EDI

eIDAS[39] stands for 'Electronic Identities And Trust Services'. Through eIDAS, European member states have made agreements to use the same concepts, levels of assurance[40] and digital infrastructure. Part of the Regulation relates to the cross-border use of EU qualified login schemes. This can only be done with a reliable online identity check at the front door. The eIDAS Regulation applies to public organisations and private organisations with a public service role. They are obliged to accept EU qualified login schemes within digital services. The duty under eIDAS applies to organisations that use DigiD and eHerkenning.
When eIDAS was introduced, SURF informed institutions about what eIDAS would mean for their institution, and a wiki FAQ is available here: https://wiki.surfnet.nl/display/eIDAS/eIDAS+Home.

In a project that goes by the name European Digital Identity (EDI), the European Commission is working to expand the existing Regulation, including extending the European digital identity beyond the public sector and regulating the use of 'attributes'.[41] Initiatives around the 'European Identity Wallet' are also emerging from this.

### Digitale bronidentiteit (DBI) - burger [digital source identity - citizen]

This is a citizen's digital identity issued, recognised and enshrined in legislation and regulations by the Dutch government. The digital identity is intended for use in the public and private sectors. This digital source identity contains an identity dataset required to participate in society. Through the digital source identity, the government will create an 'authoritative source' of trustworthy identifying data. This will provide a key generic baseline for trust in the digital world. As an 'authoritative source', the DBI[42] will enable derived digital identification means, just as with a physical passport, to be used to enable other derived identfication means.

### Virtual identity document (vID)

A vID is the digital version of your familiar passport or ID card in the form of an app on your smartphone. In the future, this digital identity will have to meet the same trustworthiness requirements as your passport and identity card currently do for use in both the physical and digital world. The Experiencelab vID was launched in September 2020. This is a collaboration between various government organisations, industry and other organisations, including RvIG, Digicampus and TNO. The aim of the lab is to test various use cases with vIDs being issued by a local authority. They are also investigating a number of applications using the vID:

- Online check-in and border control with a vID at an airport
- Online age check using a vID in a webshop
- Identification on the street using a vID

### IRMA

IRMA stands for 'I Reveal My Attributes' and was developed by the Privacy by Design Foundation established by Professor Bart Jacobs in Nijmegen. IRMA allows users to disclose part of their identity online to parties and add a digital signature in a way that is secure and protects privacy.

[38] For a recent overview, see https://zoek.officielebekendmakingen.nl/blg-1002922.pdf
[39] Source: https://www.digitaleoverheid.nl/dossiers/eidas
[40] Source: https://afsprakenstelsel.etoegang.nl/display/as/Technische+specificaties+en+procedures+voor+uitgifte+van+authenticatiemiddelen
[41] Source: https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:52021PC0281&from=NL
[42] Source: Samenwerken aan een digitale bronidentiteit - Digitale Overheid

As part of a pilot project, the municipality of Nijmegen has enabled a group of residents to retrieve their data from the Personal Records Database and to use it for their 'digital identity' in the IRMA app ('I Reveal My Attributes'). Logging in with IRMA means the person no longer needs to create user profiles on each of the websites and apps they use. With IRMA, websites only receive the data from the user that is actually needed. They can be sure that this information is trustworthy as it comes from an official source. The Privacy by Design Foundation has a partnership with SDIN (administrator of the .nl domain) and is also responsible for the administration and maintenance of the IRMA technical infrastructure.

### Decentralized Identity (DCI) / Decentralized Identifiers (DID)

DCI/DID provides an alternative to centralised IAM architectures by establishing trust in identities and resilience across the system as a whole, with little dependence on centralised parties or identity sources. DCI/DID offers an alternative approach that is free from the security, privacy, and usability concerns associated with traditional, fragmented approaches to digital identity. DCI/DID gives users control over their identity and data, allowing service providers to communicate with users faster and with greater confidence. In the current situation, providers tend to hoard identity data relating to users. Using DCI/DID enables identity and service providers to improve security and ease of access for end users, while reducing exposure to data theft and potential breaches of privacy legislation. A working group is active within w3c to develop the standards for DID[43]. Parties already significantly involved in developments in the field of DCI/DID include IBM and Microsoft. They also use the identities within their eco-systems as an identity provider for other environments.

### IDunion

The IDunion Indy network project was launched in the European Union (EU) in April 2021. IDunion started a test network in early 2021 and has the funds to launch the IDunion MainNet later in 2021. The aim of the IDunion network is to support only users in the EU in recording transactions as a counterpart to Sovrin and Indico, which are focused primarily on the US. The verifiers could of course be based anywhere, so that anyone in the world will be able to read from the IDunion ledger. The concept of national/regional Indy networks stems from the idea that, as the use of verifiable references becomes ubiquitous, the trustworthiness of general ledger assistance programs becomes a critical aspect. Since the availability of ledgers is critical when they are in wide use, they should be part of a country's critical infrastructure alongside the Internet, emergency phone numbers (e.g. 911 or 112), the electricity grid, etc. Other countries have also started to explore possibilities for creating their own ledger.

[43] https://www.w3.org/2019/did-wg/

# Annex G: Points for attention

During the inventory phase of generating the domain architecture, various problem areas and developments were identified through interviews, reports and sessions. A description of the most important points for attention is provided below.

### Guest access

It is difficult for lecturers and researchers to grant guest lecturers, fellow researchers or others access to their teaching or research via the institution's digital services. This is often resolved at institutions by creating a 'not on payroll' registration in HRM for guests, which automatically creates a 'guest' account. A federated link for 'guests' can be set up via SURFconext. Generally speaking, the biggest challenge is authorisation for such 'guests'. SURFconext often provides the identities of users to other institutions, or (via eduID) the identities of 'guests', potentially 'the whole world'. Sometimes collaborations with other foreign institutions are also desirable.

### National focus

European collaboration in education is difficult because it is not possible to share educational data with other (European) institutions due to the lack of standards and agreements.

### Focus on own institution

Studying or working at different institutions usually requires the user to have a separate ID for each institution where they study or work. The current IAM facilities are primarily focused on the individual institution. Studying and working at different institutions requires user IDs that can be used across the sector, such as eduID.

### Collaboration with parties outside the higher education sector

Collaboration with controlled access to applications and information sharing between an institution and organisations outside the higher education sector (companies, publishers, national government and hospitals or institutions in primary education, general secondary education and vocational secondary education) is challenging in the current situation.

### Data protection and convenience

The Studielink number is used in the higher education sector for a number of chain processes, but not all chain processes. One of the reasons for this is that, under the GDPR, it is undesirable for the same central education number to be used and stored multiple times with the various parties in the chain. For this reason, preference is given to working with pseudonyms issued by a party that can be regarded as 'trustworthy' or to use polymorphic pseudonyms or other techniques without a trusted party. Such a solution potentially involves much greater complexity, and it is important to consider carefully whether its use is justified by the problem. From the point of view of the citizen or student, it is desirable to make the system as easy as possible without jeopardising the individual's privacy.

### Enrolment process for foreign students

Foreign students are verified at the institution level when they enrol, which creates a lot of extra work and can produce varied outcomes. Studielink recognised this as an area requiring attention. A process for the Digital Verification of Personal Data is now up and running, and works for 60% of international students.

### Quality assurance

Institutions do not have any way of objectively demonstrating to partners and third parties the degree to which they are able to properly manage identities and grant rights.

### Unwanted lock-in

A commonly held view within the sector is that institutions and education are disappearing entirely into the cloud environments of providers without a second glance. These environments have their own integrated digital cloud identity that gives access to a large number of applications. In that situation, institutions are not able to change their identity and access provider without major impact and inconvenience in terms of the provider's cloud application. This becomes a problem when the institution wants to change providers, because there is a sort of linked provision of different combined services. Institutions are then strongly dependent on the provider's roadmap.

# Annex H: Definitions and terms

An explanation of the definitions and terms that appear in the domain architecture is given in this annex. A number of terms are taken directly from a source, and this is indicated with the term. General terms are based on the IAM terminology from the Nederlandse Overheidsrefentie-architectuur (NORA) [Dutch government refence architecture]. Terms that relate specifically to virtual credentials have been taken from the W3C standard for verifiable credentials (VC Data Model).

- ***Attribute:*** a unique characteristic or data item of an entity (source: NORA)
- ***Authentication:*** a process that enables the identification of a natural or legal person, or the origin and integrity of data in electronic form, to be confirmed. (Source: NORA)
- ***Means of authentication:*** a means by which authentication of a user can take place. (Source: NORA)
- ***Authentication factor:*** a factor that has been confirmed to be linked to a person and falls into one of the following three categories. • Ownership-based authentication factor: an authentication factor that the individual concerned must demonstrate is in their possession. • Knowledge-based authentication factor: an authentication factor that the individual concerned must demonstrate they have knowledge of. • Inherent authentication factor: an authentication factor based on a physical characteristic of a natural person such that the individual concerned must demonstrate that he or she possesses that physical characteristic. (Source: NORA)
- ***Authorisation:*** authorisation is the process of establishing the mandate held by an authenticated identity and the rights associated with this mandate. (Source: NORA)
- ***Level of assurance:*** the degree to which trust can be placed in a means of identification. (Source: NORA)
- ***Source identity:*** a source identity (or basic identity) is the identity of a (legal) person, as currently defined and formulated by a government agency via means of identification (identity documents), that can be used to participate in society (passport, identity card or driving licence, potentially including other means in future). (Source: NORA)
- ***Claim:*** A *claim* is an assertion made about a *subject*. A *subject* is a thing about which claims are made. Claims are expressed as a relationship between a subject, property and value. In the data model, a strong and diverse set of claims can be built up. These can be single claims or composed of several inter-related claims in the form of a *graph*[11]. (Source: Verifiable Credentials data model)
- ***Credential:*** A credential is a set of one or more *claims* made by the same entity. Credentials may also contain an identifier, as well as metadata that describes the properties of the credential, such as the *issuer,* the expiry date, a public key for the purposes of verification, the revocation mechanism, etc. The metadata can be signed by the *issuer.* A *verifiable* credential is a set of claims that are tamper-proof, linked to metadata and cryptographic proof about *the issuer,* such as a digital signature. (Source: Verifiable Credentials data model)
- ***Digital/electronic identification means:*** a tangible and/or intangible unit that contains personal identification data and is used for authentication in an online service. (Source: NORA)
- ***Digital/electronic identity:*** an identity for use by entities in the online world. A digital identity can be made up of various aspects (attributes) that are held on record about a particular entity. ISO/IEC states: a digital identity is a set of attributes that can be related to an entity. (Source: NORA)
- ***Digital/electronic identity infrastructure:*** the entirety of systems, agreements, standards and services relating to the digital identity of (legal) persons. (Source: NORA)
- ***eID:*** eID stands for Electronic Identification. (Source: NORA)
- ***eIDAS:*** eIDAS stands for Electronic Identification (eID) and Trust Services (AS). This is an initiative of the European Commission that has the aim of making electronic interactions between enterprises, citizens and organisations more secure and more efficient, and enabling all EU countries to recognise one another's eID and AS. (Source: NORA)
- ***Federated Identity Management:*** the provision of the processes, agreements, standards and technology that make it possible to share digital identity and context data in a controlled way across (shared/joint) institution boundaries

- ***User:*** anyone who is familiar with and uses a service or facility. Users could include the following:
  - *Student, employee, educational professional, researcher, alumnus:* a natural person from an institution who has one or more relationships with the higher education sector with a unique identification
  - *Partner:* a natural person from a partner organisation (not in the higher education sector) who has one or more relationships with institutions within the higher education sector with a unique identification
- ***Authoritative source:*** any source, of whatever kind that can be expected to provide accurate data, information or evidence to be able to demonstrate an identity. (Source: NORA)
- ***Higher education card:*** set of features that make a higher education user uniquely recognisable in certain contexts within the higher education sector for digital identification
- ***Holder:*** the role played by an entity in holding one or more verifiable credentials and generating one or more verifiable presentations from them. Examples of *holders* include students, employees and customers. (Source: Verifiable Credentials data model)
- ***Identification:*** the process of making an identity known. (Source: NORA)
- ***Means of identification:*** (physical or digital) device by which the person for whom it was issued can identify him or herself. (Source: NORA)
- ***Identity:*** an identity consists of the registered aspects (attributes) that determine to a sufficient degree who or what someone or something is. (Source: NORA)
- ***Identity provider:*** an organisation or service that vouches for the identity and context data of a user who requests access to an application within the higher education sector
- ***Issuer:*** the role played by an entity in asserting claims about one or more *subjects.* (Source: Verifiable Credentials data model)
- ***Legal identity:*** a legal identity (or statutory identity) is an identity that is defined and regulated by law. (Source: NORA)
- ***Personal identification data:*** a set of data used to establish the identity of a natural or legal person or a natural person representing a legal entity. (Source: NORA)
- ***Registry holder:*** a party that registers data such that it constitutes an authoritative source. (Source: NORA)
- ***Self Sovereign Identity (SSI):*** The concept of Self Sovereign Identity locates control and power over a digital identity fully with the entity that this digital identity represents. This requires complete independence from a central registry or central authority. (Source: NORA)
- ***Subject:*** an entity to which claims relate. Examples include people, animals and things. In many cases, the holder of a verifiable credential is the *subject*, but this is not always the case. For example, a parent may hold the verifiable credentials of a child (the *subject*) as the *holder,* or the owner may hold the verifiable credentials of a pet (the *subject*) as the *holder.* (Source: Verifiable Credentials data model)
- ***Verifier:*** A role that an entity performs by receiving one or more verifiable credentials, optionally inside a verifiable presentation, for the purposes of processing. Examples include employers, security administrators and websites. (Source: Verifiable Credentials data model)
- ***Verifiable data registry:*** a role that a system can fulfil by mediating in the creation and verification of identifiers, keys and other relevant data, such as schemas for verifiable credentials, revocation registries, public keys of issuers, that are required for the use of verifiable credentials. Such registries may include trusted databases, decentralised databases, national identity registries and distributed ledgers. An ecosystem will often have different types of registries containing verifiable data
- ***Verifiable presentation:*** displaying data from one or more verifiable credentials in such a way that the origin *(authorship)* of the data can be verified. Verifiable presentations may be exactly the same as verifiable credentials in all respects, but can also contain data derived from credentials in a way that is cryptographically verifiable. In the latter case, the verifiable credentials themselves are not part of the verifiable presentation. As with verifiable credentials, metadata and evidence are an integral part of the verifiable presentation.