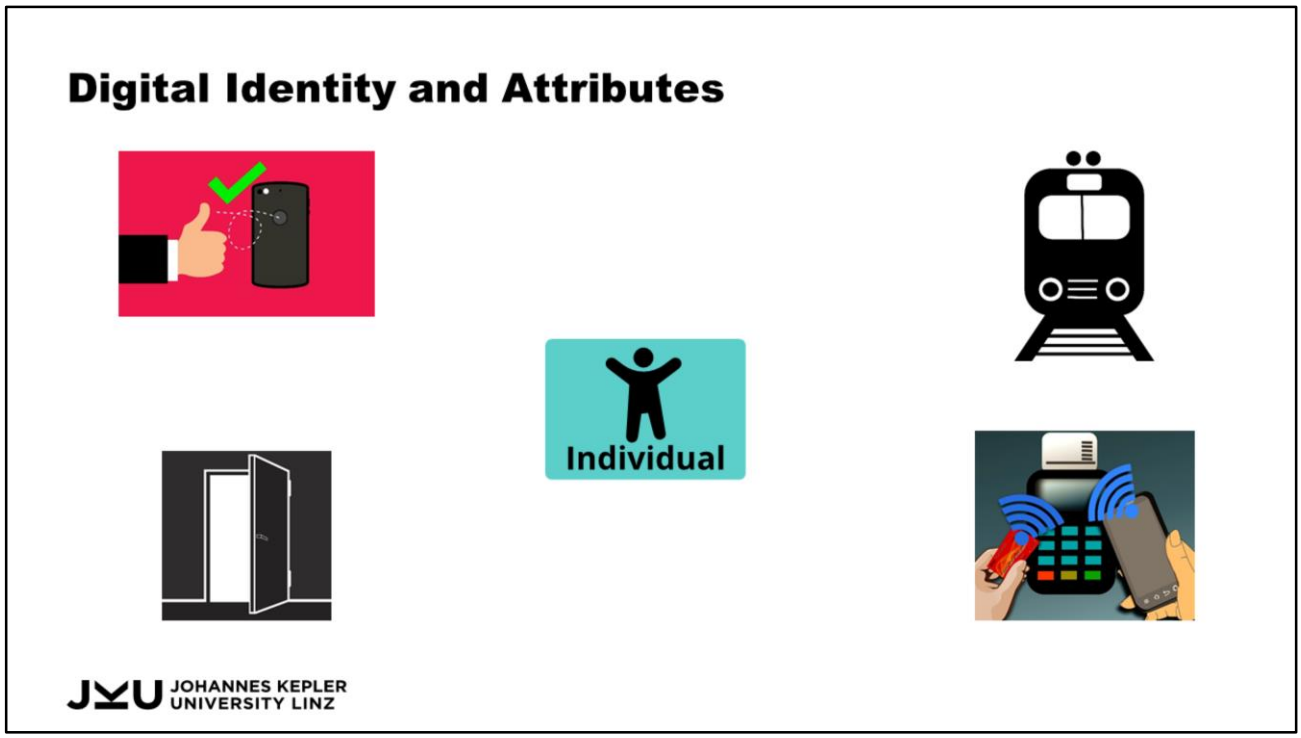
Thank you for the opportunity to represent some aspects of the excellent research happening in Upper Austria for this august round. As you can probably imagine, we are currently thrilled and in intense discussions about the intended establishment of a new Technical University. We happily take on the challenge to create a new cornerstone of Austria's academia, augmenting the long history of existing institutions.

I was asked to talk about the "mission and use of science with relation to policies and the global crisis". This is an interesting question, and I'll try to do my best to answer it at the end of my short keynote. The first counter-question, however, is "which of the crises"? As I unfortunately have little to contribute to the ecologic and climate crisis, I will focus more on the two crises of the Covid-19 pandemic and information systems security – especially the rampant abuse of personal, sensitive data – and how I see them to be interlinked. This is the part where I talk about my current scientific area of research ☺

Any secure communication, for example instant messages, voice or video calls, or a remote bank transaction, require a form of digital identity. That is, some form of identifier such as a user name or phone number and proof that an individual actually owns this digital identity. Providing such proof is typically called authentication.



When we think about authentication, what might come to mind is our laptop and desktop computers or our smartphones. Entering that PIN or password or using our fingerprint, face, iris, or other biometric authentication when we unlock the screen again is happening so often that it has already become second nature. But digital identity is so much more these days.

We are opening doors with NFC plastic cards or tokens and use RFID chips in passports,
we pay wirelessly with NFC credit or debit cards, and
we use digital tickets for public transports as part of our daily lives.

All these examples rely on different so-called attributes like our fingerprint patterns, the permission to access a particular door, our account balances, or possession of a valid month or year pass for public transport. However, we never use all these attributes that describe aspects of our digital life at the same time. For entering an underground train, you shouldn't need to transmit your full name, place of residence, account details, or your apartment door keys. We pick and choose which aspects of ourselves we present in which situation.

But what does it actually mean in practice?

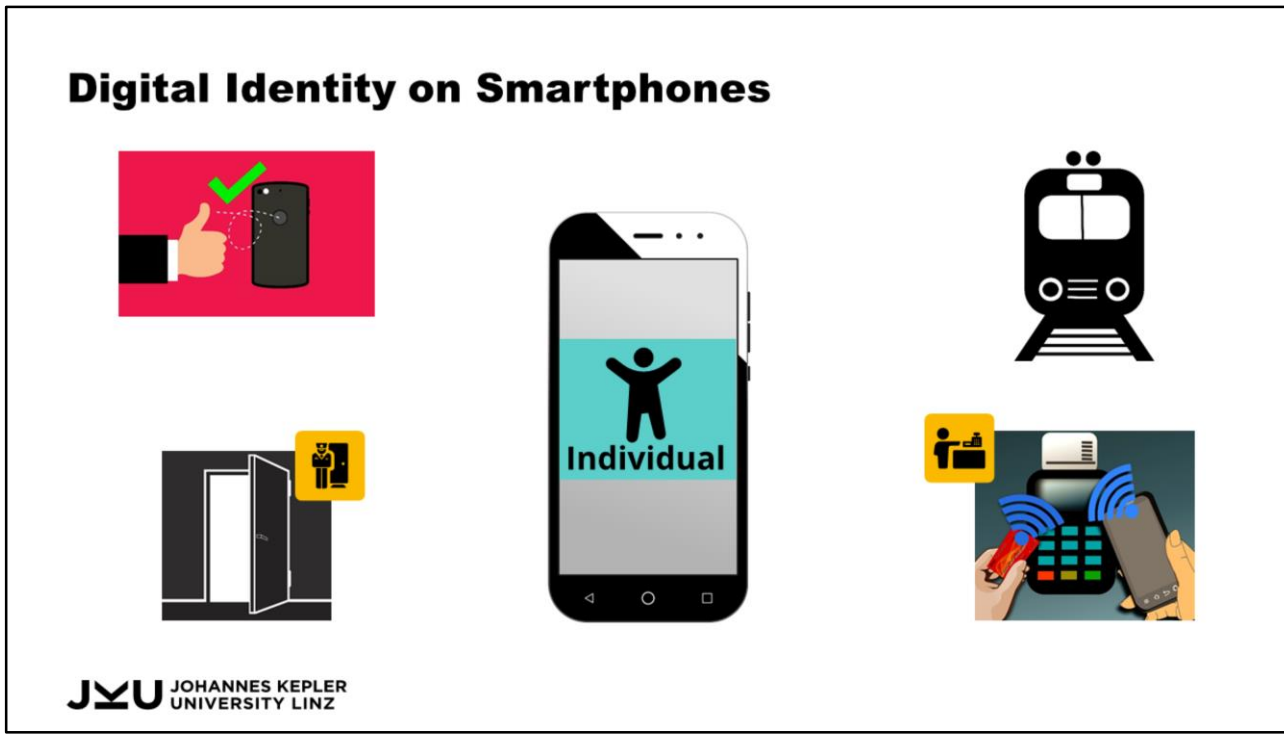
Digital Identity – “State of the Art”

JOHANNES KEPLER UNIVERSITY LINZ

Right now, on the web or our smartphones with specific apps, we still tend to juggle with a multitude of independent accounts. Putting on my security lecturer hat, I of course have to repeat the scientific wisdom to use a unique and sufficiently strong password for each of them.

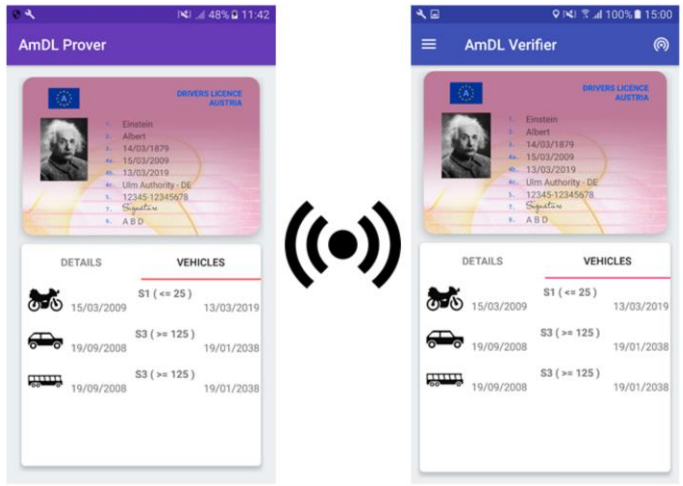
However, we also know from scientific research that most people – myself very much included – have trouble remembering around a Hundred different passwords, some of which we only use about once a year for submitting tax reports or created on the spot for the restaurant’s contact tracing list. That is, passwords don’t tend to work well for one-time use accounts.

On the other hand, physical world interactions that require authentication like entering a building or crossing a country border still require separate physical access cards and documents to be carried.



That is one of the reasons why our digital identities are already moving onto our mobile phones. We can use the phone itself as a password manager, to unlock building doors and cars, pay wirelessly, and use transport ticket apps. One bridge between the physical world of interactions and the digital world of attributes is to keep them all on **the** single device that we seem to be physically carrying anywhere anyways.
Unfortunately, this increased use of data on consumer devices brings us directly to the current crisis of bad IT security and abuse of personal data. Luckily, we can do better, and scientific results have already started to influence the direction of mobile identity for better security and privacy.

Scenario 1: Traffic Check



All attributes are transferred

- Name
- Date of birth
- Nationality
- (optional) Place of residence
- (optional) Biometric features
- (optional) Place of residence
- Vehicle classes, potential restrictions, …

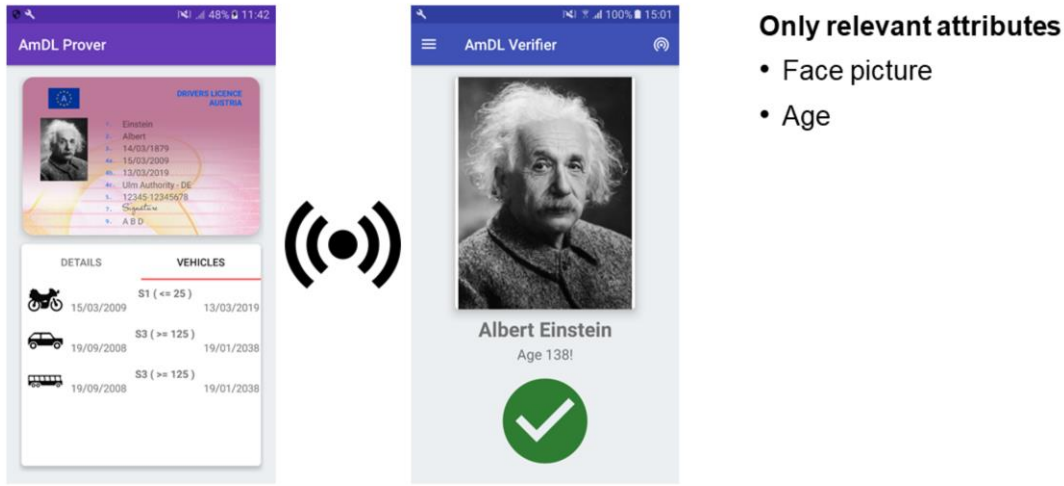
Also needs to work offline!

JOHANNES KEPLER UNIVERSITY LINZ

One example is a mobile driving license – or in the slightly farther future, a mobile passport – which combine a set of highly useful attributes and are issued by a government agency. For a traffic check conducted by a police officer or a border crossing, all of those attributes are transferred and verified, including full name, date of birth, a face picture in high resolution, potentially a place of residence, other biometric features, and driving license or passport specific data.

As there are still some places on Earth that don't yet have solid network connectivity – including exotic places like tunnels or parking garages –, this should still work when the phones are offline. From a research point of view, that alone poses a number of interesting challenges.

Scenario 2: Proof of Age



Only relevant attributes

- Face picture
- Age

JOHANNES KEPLER UNIVERSITY LINZ

As the driving license or passport are widely available, government issued documents, they are also used for many other scenarios outside their original purpose. However, for cases like age verification, most of the included attributes are not actually necessary for the interaction. For entering a club or buying alcohol, it shouldn‘t be necessary to transmit our full name, place of residence or the fact that we might be required to wear glasses to drive a car. Yet handing over one’s physical driving license to a bouncer or sales person does exactly that. That‘s the first case where a digital version can provide much better privacy guarantees than the physical version of the ID. Selecting the age verification profile on the holder’s device will only transfer the face picture and age – not even the full date of birth – in such a case, and nothing else.

Scenario 3: Public Transport

Image credit: https://pixabay.com/photos/underground-tube-map-stations-2725336/

Location traces constitute highly sensitive data

- Place of residence / work
- Religious beliefs
- Illnesses
- Hobbies, particular preferences

Only relevant attributes

- Place of entry / exit **or**
- Possession of time based ticket

But no unique identifier!

JOHANNES KEPLER UNIVERSITY LINZ

Another example is using public transport: Even when not linked to a name and therefore sometimes called anonymous, location traces are highly sensitive data. From the places an individual visits during their days, it is often trivial to determine not only their place of residence and work, but also religious beliefs, illnesses, hobbies, or other particular preferences. Scientific research has made it clear for over a decade that de-anonymization or re-linking of data traces is often very easy and that existing policies for anonymizing data are not sufficient.

Transmitting a complete location trace to pay for the use of public transport with our smart phones therefore seems wildly out of proportion. With a well designed digital authentication system, that also isn't necessary. The only relevant attributes are the place of entry and exit for a particular journey or even better a proof of possession of a valid time based ticket such as a monthly subscription pass.

Scenario 4: Contact Tracing

Location traces constitute highly sensitive data

- Place of residence / work
- Religious beliefs
- Illnesses
- Hobbies, particular preferences

Only relevant attributes

- Contact with (pseudonym) person X for Y minutes on day Z

But no unique identifier!

JOHANNES KEPLER UNIVERSITY LINZ

Now is a perfect time to talk about the second crisis, which is the one on top of most people's minds, because this is also about location.

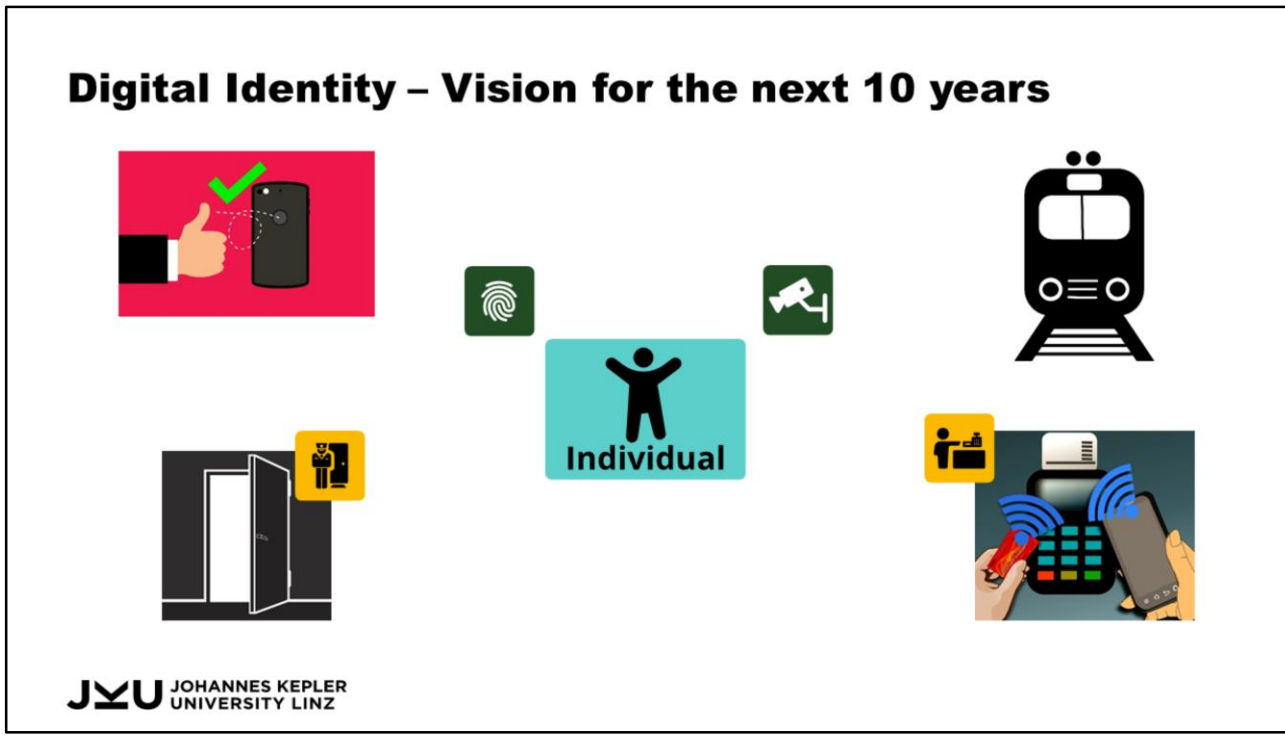
Contact tracing is one tool for mitigating pandemic virus spread like the current Covid-19. In this case, the relevant attributes are that a contact has happened with a pseudonymous person X for Y minutes on a day Z, and nothing else. The complete location trace throughout the day is not required and can be dangerous if leaked and abused. I am very happy that, in this case, scientific results on the balance between privacy and utility for contact tracing have been directly and quickly used to shape policy, and most countries that have a mobile contact tracing app do so with data minimization. Rapidly rotating pseudonyms are exchanged through local radio channels – specifically Bluetooth Low Energy – and stored in a decentralized manner only on the smart phones involved in a particular contact. Others are unable to link those pseudonyms when no infection occurs. This allows to tackle one crisis – the pandemic – without making the other one – abuse of personal data – any worse.

Digital Identity on Smartphones

JOHANNES KEPLER UNIVERSITY LINZ

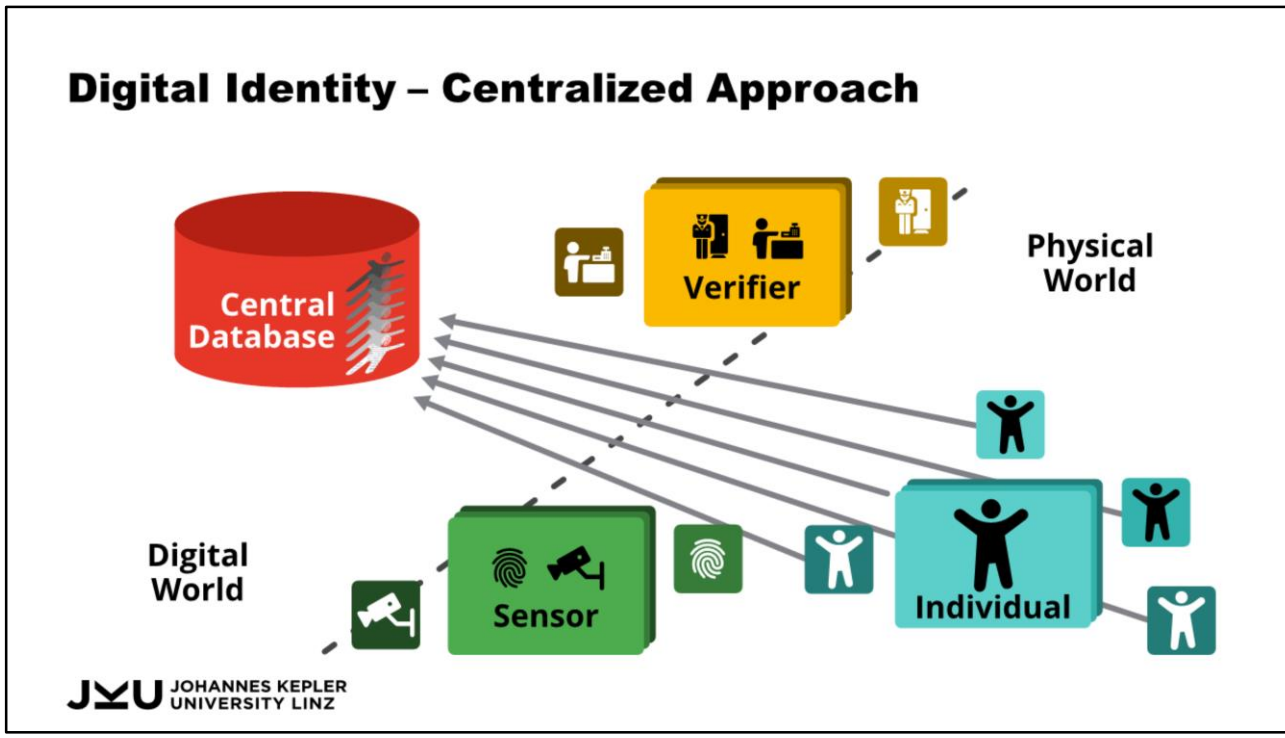
If we think further ahead – maybe 5 to 10 years –, we predict digital identity to move from phones even more into the environment, the cloud.

One technique that offers a way to bridge usability, security, and privacy, is **biometric authentication**.

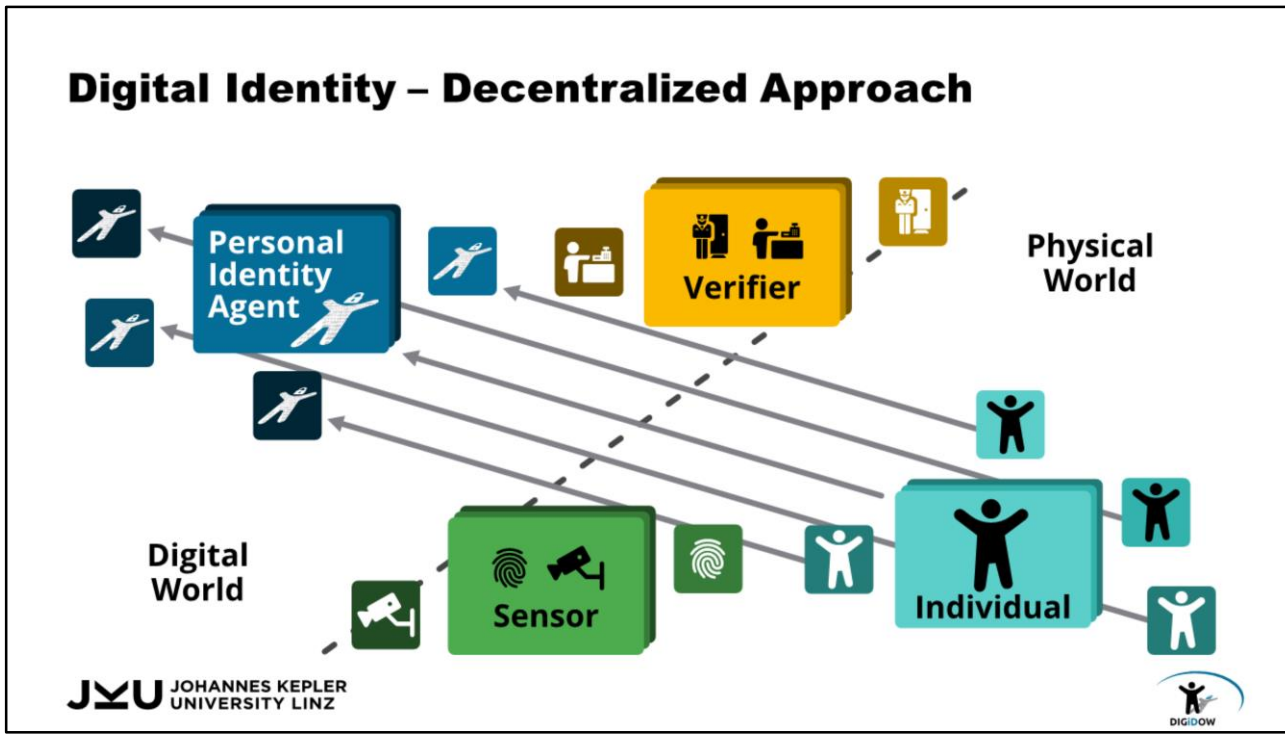


Using various sensors, an individual‘s fingerprint, face, voice, iris, gait patterns or many other biometric features can be used to identify that individual. The often-portrayed vision is that we should be able to walk through the world without having to carry any physical keys, documents, or remember other forms of identification. What we don’t have to carry can’t be broken, lost, or stolen.

There are different way to implement such biometric digital identity:



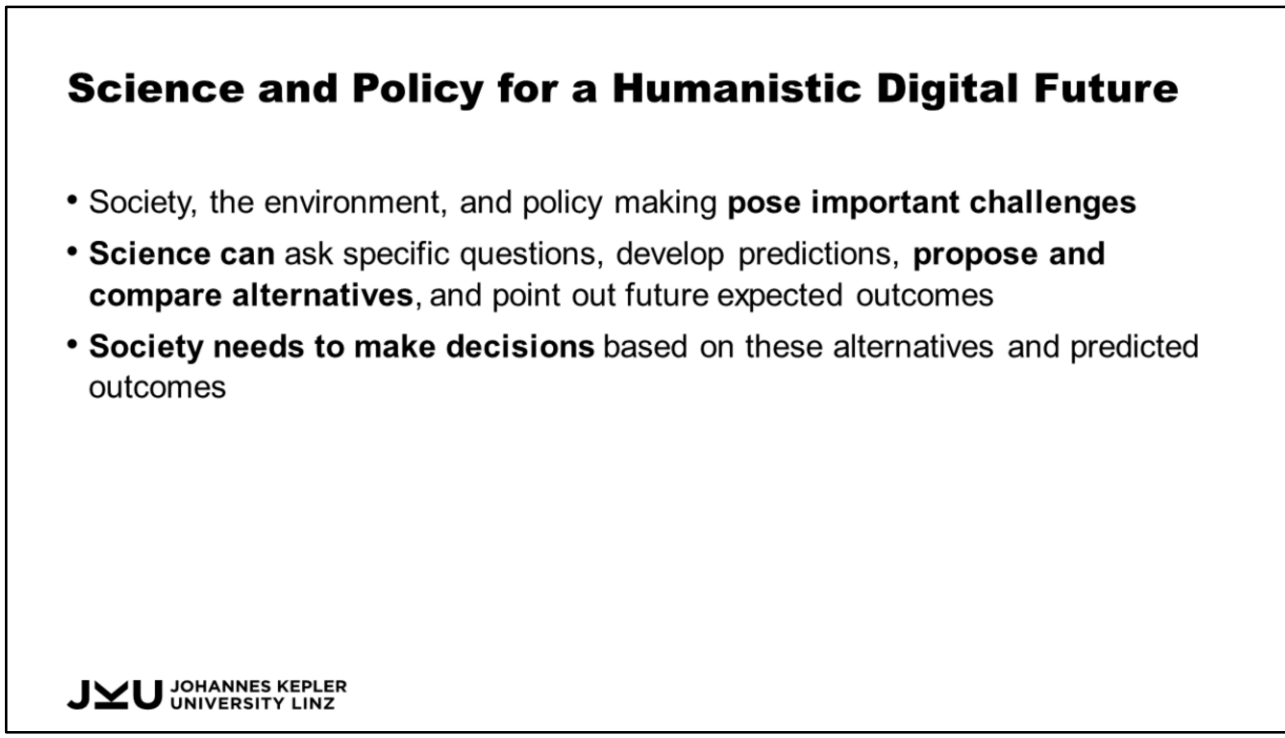
The obvious and technically simpler approach is the use of **centralized** databases. All biometric features and relevant identity attributes can be stored and linked and queried from there when crossing a country border or entering public transport. The Aadhaar system in India with centralized biometric data of over 1.2 Billion citizens has been the largest example of this approach since 2016.



The second option is a **decentralized** approach, to assign each individual a personal proxy, a so-called Personal Identity Agent or PIA. This remains under the possession and control of that individual. The owner can decide where to execute this agent, for example on which cloud provider or on a smart phone. Moving the agent from one host to another should be as simple as keeping multiple copies for better availability, which is directly within the spirit of modern and highly influential regulation like the GDPR. Both the centralized and decentralized approaches have their own advantages, but also their own challenges. Before deciding on one approach, both need to be analyzed and compared systematically.

In the nationally funded Christian Doppler Laboratory for Private Digital Authentication in the Physical World (CDL Digidow), we are analyzing and building prototypes for the non-obvious decentralized approach, directly here in Linz, but with an aim of potential global deployment. All results will be published and code will be released as open source to share with the world.

This is where I end the excursion into my own pet topic of scientific research and come back to try and answer the original question.



What can science do for society to help deal with such crises?

Our environment, society, and the rules and policies that regulate it, regularly pose important challenges that need to be solved. Sometimes, those challenges even manifest themselves as crises such as the Covid-19 pandemic or rapid climate change.

The main use of science for those challenges is to ask the right questions and come up with potential solutions. Typically, there will be multiple alternatives. Science can and should propose and analyze those alternatives. Science can predict expected outcomes when taking one of those alternatives; it can prepare for decisions based on fact or at least state-of-the-art theory. But science does not make policy decisions.

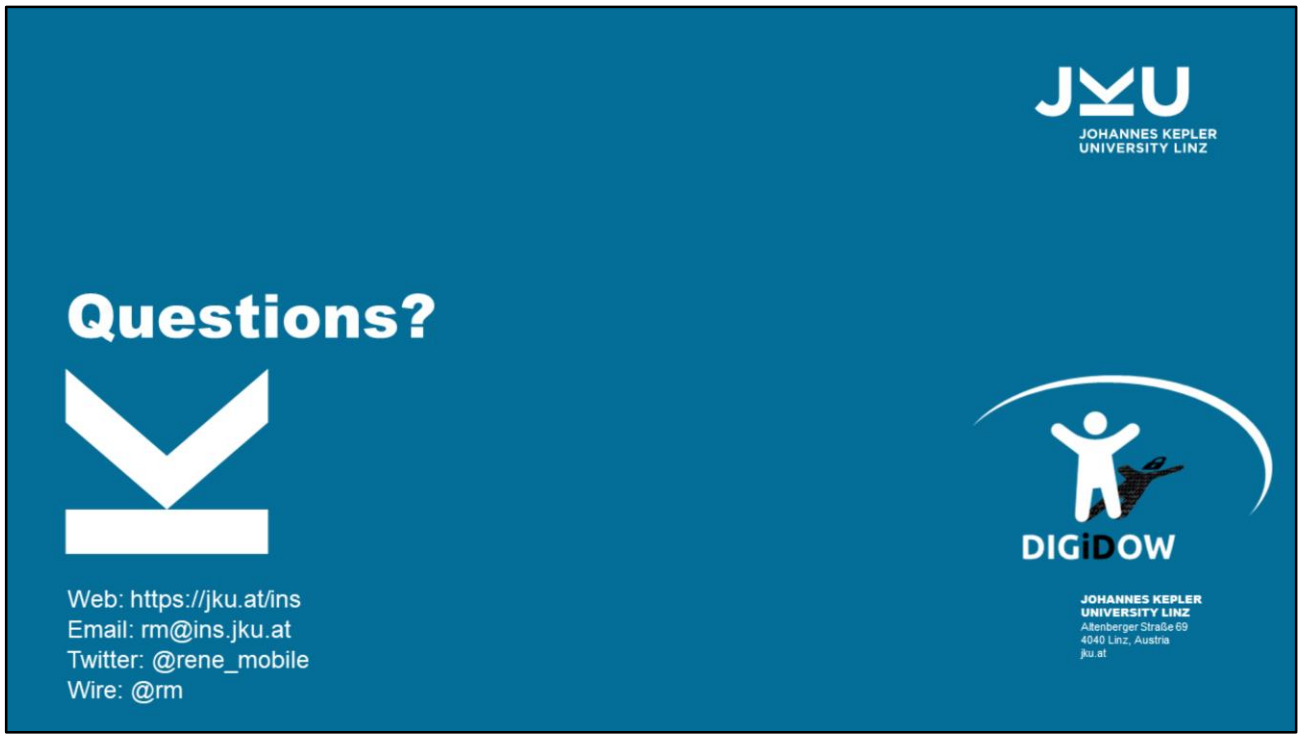
Those decisions need to be made by the whole society and executed by policy making.

Covid-19 was and still is a prime example of how such interaction can work well. Predictive models of infection rates were directly used as decision helper points on a weekly basis, and in turn were and still are updated based on new data as well as changed rules of society. Contact tracing apps were made and deployed

at scale based on scientific results on how best to balance utility for society – which is mitigating the spread of infection – and privacy for individuals. We were able to deal with this crisis as well as we did so far because science and policy making tightly worked together.

Climate models have a much longer history in science. Quite unfortunately, policy has often not been based on these scientific predictions for too long, and the climate crisis could therefore act as a counter-example where science and policy have not worked together as they should. However, I am happy that we see first signs towards actions that are maybe a bit as decisive as those taken for dealing with the Covid-19 crisis, for example the EU intention to further tighten CO^2 emissions by 2030. We are still optimistic that science and policy making together will be able to address this second crisis as well.

For data security and privacy, we are still mostly at the beginning. There have been debates about data retention, new ones about face recognition and tracking of users on the web, and various smaller fires based on specific security incidents like ransomware infections. However, the big policy decision of how a primarily humanistic digital future should look like – how we are going to identify ourselves in video calls, in public transport use, in country border crossing, or in contact tracing – are still to be taken. I strongly propose that these should also be done together, to learn from what did and what didn’t work for the other crises. Science needs to point out and compare the alternatives like centralized versus decentralized handling, and civil society together with policy makers need to set the course.



Thank you very much for your attention, and I'm happy to take questions now or later through various – of course digital – channels.

Image credits

- https://pixabay.com/photos/phone-telephone-technology-business-3196540/
- https://pixabay.com/illustrations/social-networks-icons-twitter-like-1863613/
- https://pixabay.com/photos/credit-card-charge-card-money-1583534/
- https://pixabay.com/illustrations/monitor-monitor-wall-big-screen-1054714/
- https://pixabay.com/photos/camera-monitoring-minimal-1723546/
- https://pixabay.com/photos/passport-visa-border-buffer-3127925/
- https://pixabay.com/illustrations/login-register-window-button-3938429/
- https://pixabay.com/photos/private-privacy-green-secret-1647769/
- https://pixabay.com/vectors/phone-mobile-phone-internet-2903272/

JOHANNES KEPLER UNIVERSITY LINZ