



Germany's EUDI Wallet Ecosystem Development

Kristina Yasuda

SPRIND - German Federal Agency for Breakthrough Innovation

SecAppDev, 03.06.2025

Shopping & Paying via App – but IDs and Birth Certificates still on Paper

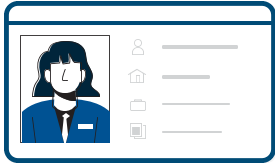
Our most important documents –
from birth certificates to ID cards –
are still based on paper and plastic.



Everything digital and absolutely secure — right?

Video/Photo identification process when opening a bank account

Hold your ID and face in
front of the camera



Recordings are
archived



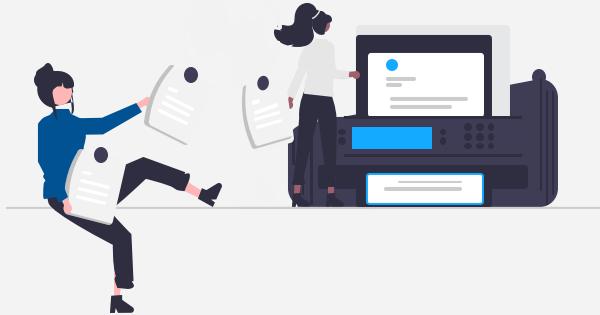
Scanned proof of
qualification for job
applications

Photographed ID card for
holiday apartment
booking



**Sending sensitive credentials
via email/messaging apps**

Challenges for Users and Services



Cumbersome - Printing on paper, manual checks, signatures, scanning – over and over again



Inefficient - Significant loss of time and inefficiency due to repetitive manual processes



Media disruptions in end-to-end processes lead to **user drop-offs**



Insufficient security features and low data quality

Digitally verifiable credentials as solution



Trust-based

Relies on trusted credential issuers who confirm specific attributes of a person



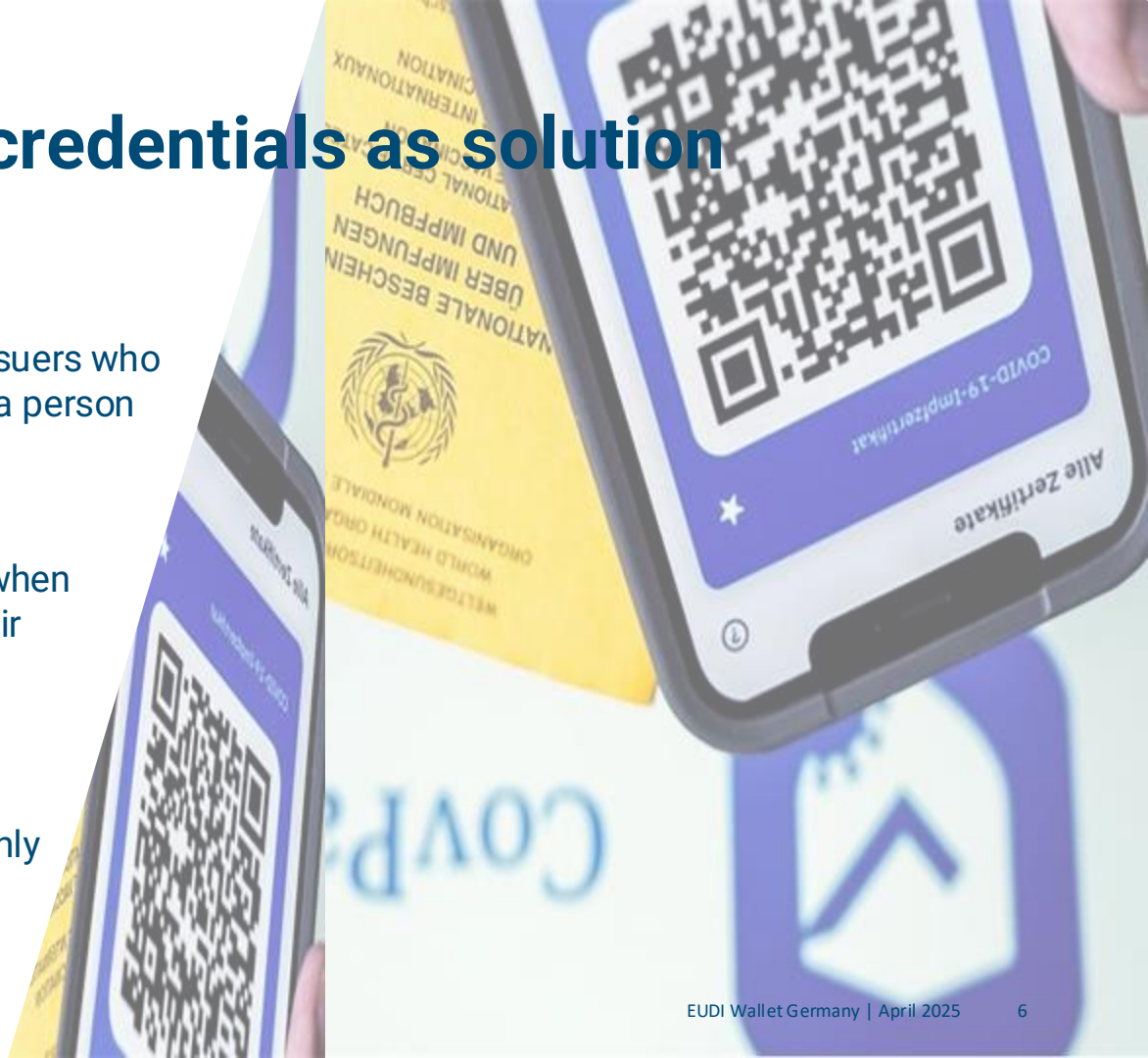
User-controlled

Users decide for themselves when and with whom they share their digital credentials



Tamper-proof & verifiable

Allows verification without unnecessary data sharing – only the essential information is transmitted.



The solution seems obvious: Wallets already exist on our smartphones



Credentials are stored digitally



Intuitive use: easy to handle, pre-installed



Accessible to many



Wallets are on our phones — but they're not yet in our control



Limited functionality: mostly for payments, flights, or concert tickets



Use cases and technologies determined by the **Providers**



Lack of influence threatens Europe's digital sovereignty



Every issuer could build their own wallet



Fragmented user experience

A separate app or wallet for every function leads to app chaos and extra effort for users



Low user acceptance

Nobody wants to download and maintain a new app for every use case



High costs

Developing, maintaining, and operating a wallet is expensive

The vision – By 2026, every EU citizen will have access to a digital wallet.

The European Digital Identity Wallet

The European Union plans to have **non-discriminatory, secure, and interoperable** wallets in place by the end of 2026.

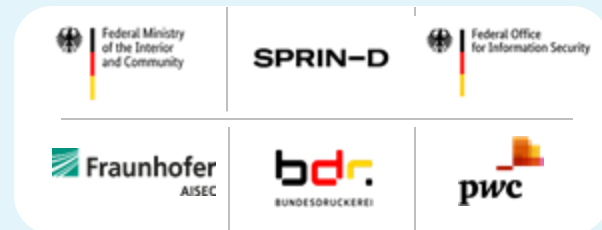
Member states can **choose** how to implement this – whether they directly provide it, mandate an entity to do so or recognize wallet solutions.

The requirement: A uniform **certification** based on common standards.



EUDI Wallet Germany

Germany is developing a secure and user-friendly wallet ecosystem through a **transparent and public architecture and consultation process**.



Germany's dual strategy: Promoting innovation while ensuring reliability

The Government-provided wallet

Ensures availability of EUDI Wallet:

Every German citizen or resident will be able to use a EUDI Wallet by EOY 2026.

Digital Sovereignty:

Germany is independent of market offers.

Basis for certification:

The Government-provided wallet serves as a 'reference model' for German certification scheme.



Open to alternative wallet providers

Freedom of choice for users:

Every user can choose from different certified and recognized EUDI Wallets.

Trust:

Users can pick the wallet provider they trust the most.

Innovation:

Competition fosters innovation (e.g. UX, form factors, additional services)

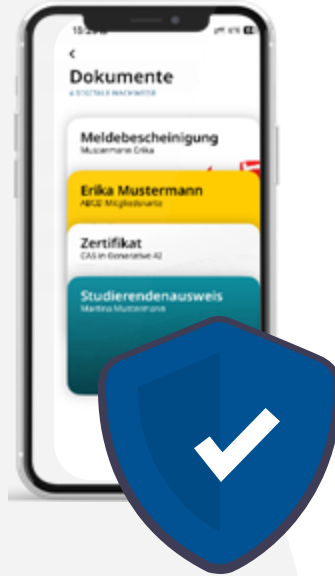
How do we guarantee digital security while ensuring sovereignty?

Strict certification of wallets

Providers must meet strict **requirements** and security standards in order to offer their product as an **'EUDI-compliant'** wallet.

Security through transparency and registration

Every service (Relying Party) that uses the EUDI-Wallet must officially register and disclose its **'Intended Use'**.



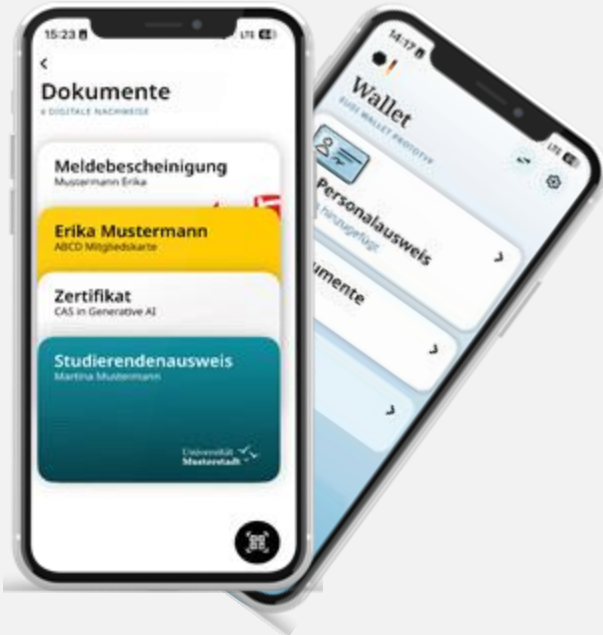
Full data control for users

Users decide for themselves which data they want to share – no transfer without consent. Credentials can be used anonymously and without traceability (**'Non-Traceability'**).

Consumer protection & complaint centers

All relying parties are listed in a **publicly accessible registry**. There are clearly defined contact points for complaints.

EUDI Wallet – More than just a digital ID



01

Identification: Secure verification using your ID card

02

Digital Credentials: Attestations of attributes: e.g., driver's license, etc.

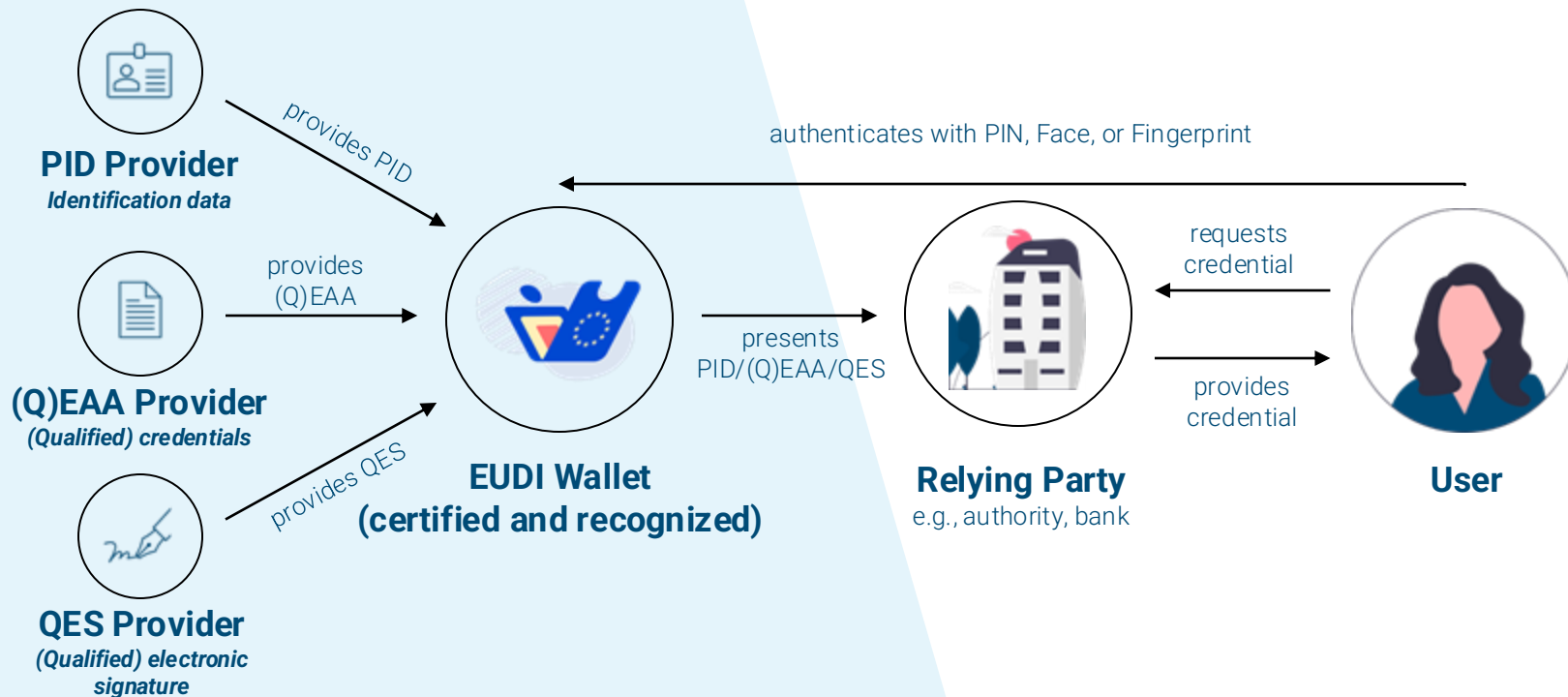
03

Electronic Signatures: Legally binding signatures without paperwork

04

Payments: Authorizing payment transactions using the Wallet

The roles in the EUDI Wallet ecosystem



The physical wallet can stay at home.



Convenience

Your wallet stays at home. Digital credentials (ID card, driver's license, health insurance card) are equivalent to their physical counterparts.



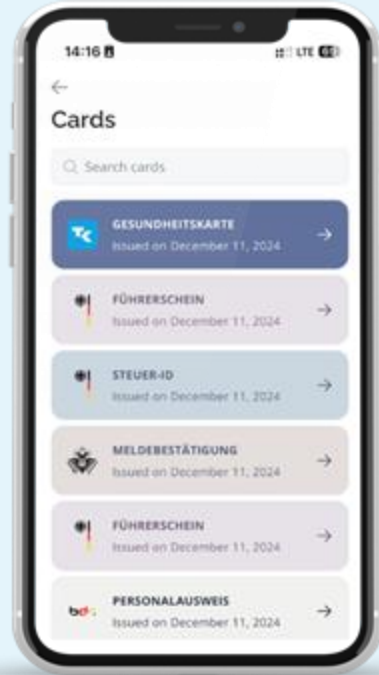
Data protection and security

Especially: Reduction of fraud and identity theft

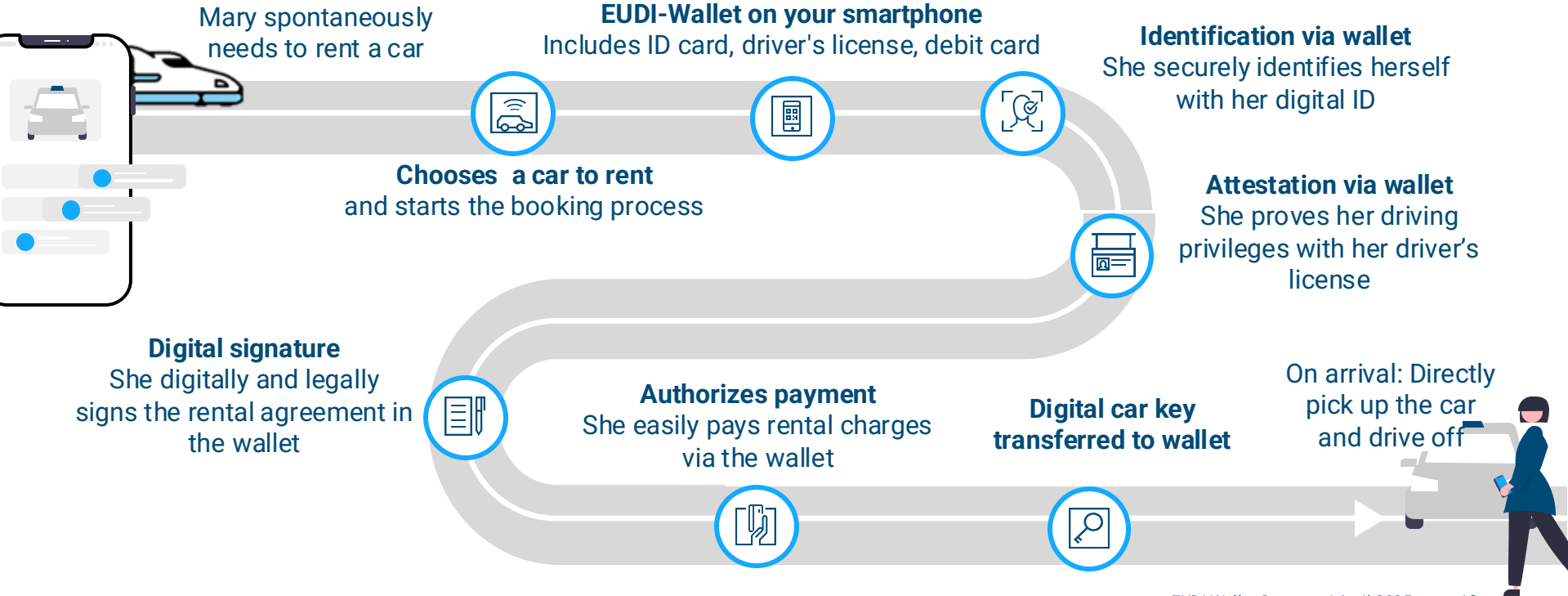


Usable anytime and anywhere

Credentials can be used across Europe both online and on-site



Renting a car easily with the EUDI Wallet



Public administration benefits from the EUDI Wallet through a unified system



Faster processes

e.g., address change notification or parental benefits application – fully digital & seamless



Efficiency

e.g., economic promotion through machine-readable, tamper-proof credentials



Increased citizen satisfaction

Through simple and straightforward access to public services



Fraud prevention

e.g., enrollment certificate and child benefits



The economy benefits as part of the ecosystem through the exploration of new markets



Growth

Through lower dropout rates (e.g., power of attorney), new products (e.g., fully digital car rental), and greater reach (across the entire EU)



Higher efficiency

Automation, support for business use cases (e.g., power of attorney), replacement of card-based solutions



Fraud prevention

Reduction of legal risks, lower costs due to reversals



New market

Trust services, technology and solution offerings for integrating the wallet into processes, alternative wallet providers

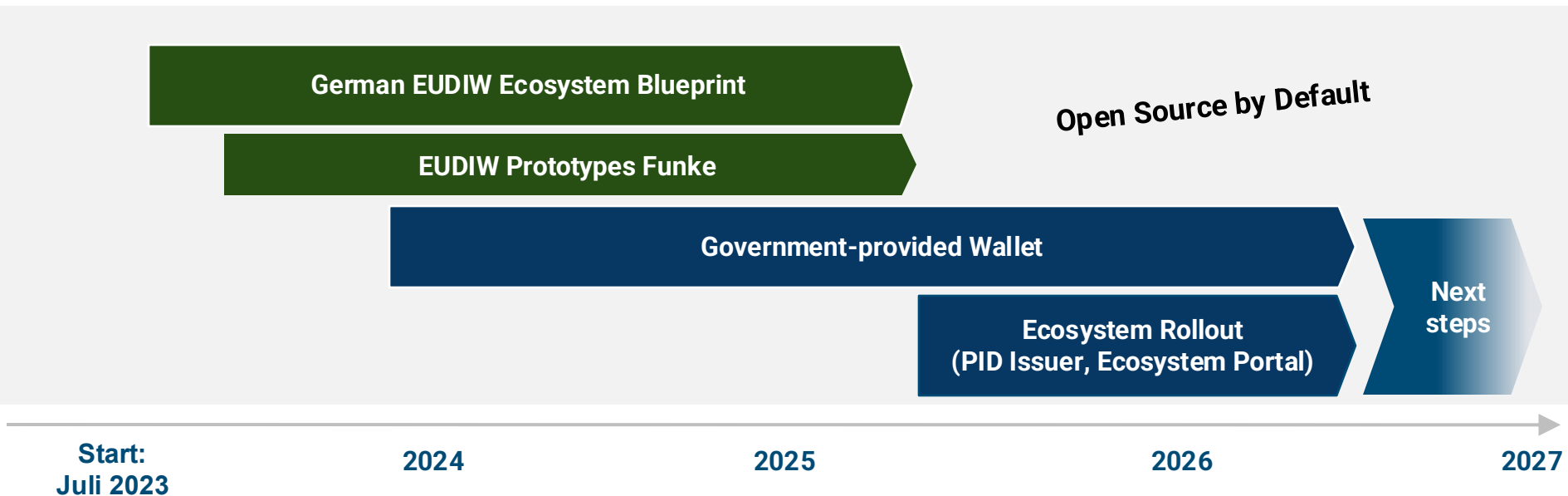


Value creation through contributions to the operation of the ecosystem

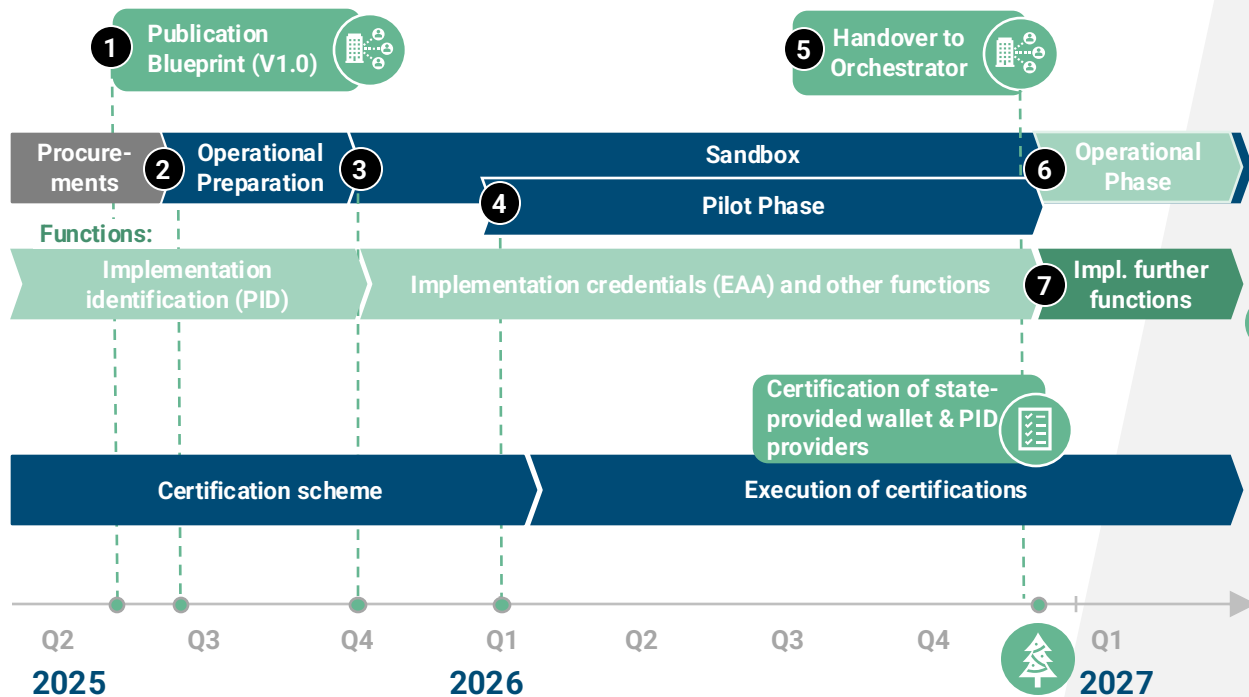
Via tenders, e.g., wallet operation



Roadmap – The path to the German EUDI Wallet



Roadmap – The way to the EUDI Wallet



- 1 Blueprint:** The overall concept for the EUDI Wallet ecosystem is published.
- 2 Procurements:** Key roles such as PID providers, wallet operators, and ecosystem management are commissioned.
- 3 Sandbox Testing Environment:** RPs can integrate the wallet in a sandbox environment. A security bug bounty program is conducted.
- 4 Pilot Phase:** All production-level processes are tested, including incident management, support recovery management, scalability, functional testing.
- 5 Handover to Orchestrator:** SPRIND hands over to an orchestrator who takes over the operation of the wallet and ecosystem.
- 6 Operational Phase:** State-provided wallet and ecosystem are rolled out to citizens and residents with PID and credential functionality.
- 7 Further Functions:** To be developed iteratively from 2027 onwards: Free electronic signature, payment authorization, pseudonym login, wallet-to-wallet use between users, forwarding & sharing of credentials.

The ecosystem behind the wallet – the key success factor is you!



Only when **all relevant stakeholders are on board – from authorities to businesses to citizens** – can the wallet be deployed successfully and nationwide!



A satellite view of Europe at night, showing city lights and the coastline, serving as a background for the left side of the slide.

From Europe to the World: EUDI Wallet as a Global Digital Identity Blueprint

1

Strategic Investment

EU focus attracts top talent, innovation, and funding — setting a pace others will follow.

2

Built for Trust

Highest security and privacy standards make the EUDI Wallet a global benchmark for trust.

3

Scalable Architecture

Architected for interoperability across 27 member states — ready for global adaptation.

4

Global Interoperability

EUDI Wallet sets a precedent for cross-border digital identity solutions.

EUDI WALLET ECOSYSTEM MANAGEMENT PORTAL

May 2025

Executive summary



The **EUDI Ecosystem Management Portal** is the **basis** for accessing the EUDI Wallet ecosystem



The portal comprises **seven core functions**, including the registration and identification of organizations to meet the new eIDAS requirements



An **ecosystem orchestrator** provides the portal for the EUDI Wallet ecosystem, a possible reuse by other ecosystems is being evaluated

An ecosystem dashboard provides a public **overview of all interactions and key KPIs**



The portal covers all **legal, technical and commercial aspects** and is the central location for all information about the ecosystem



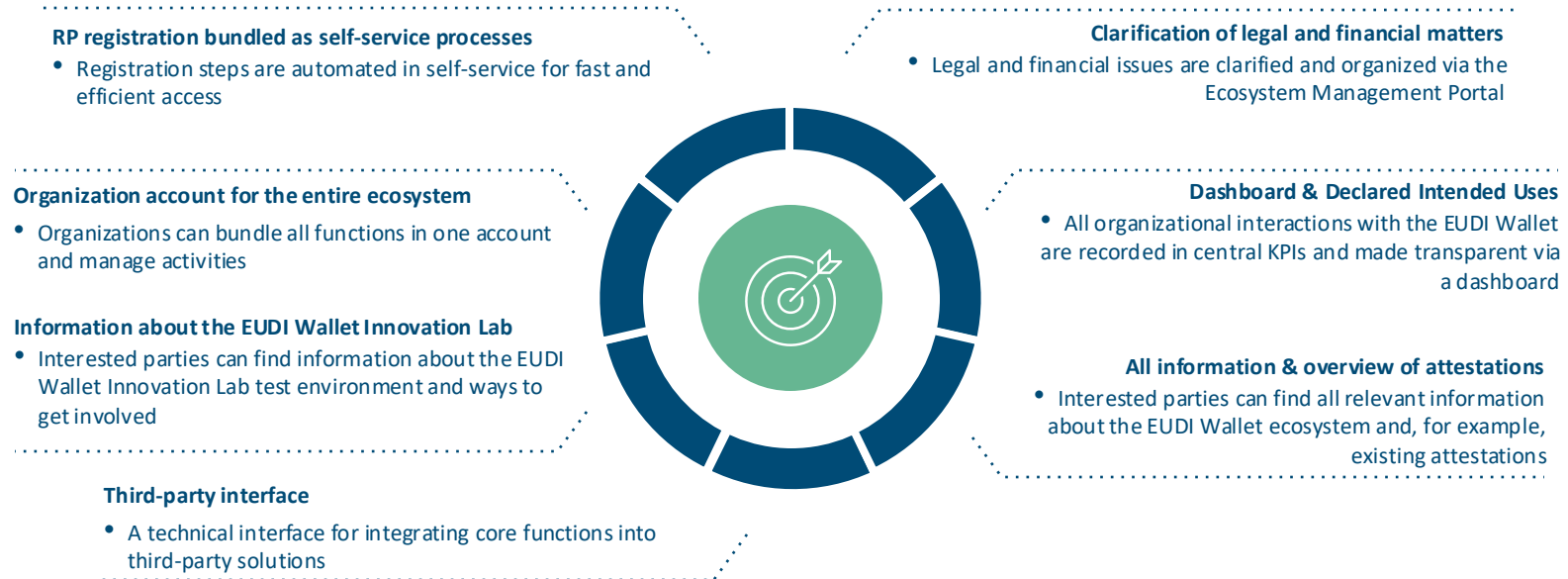
Development is **iterative** and takes place in three stages to ensure flexibility and support the ecosystem roll out



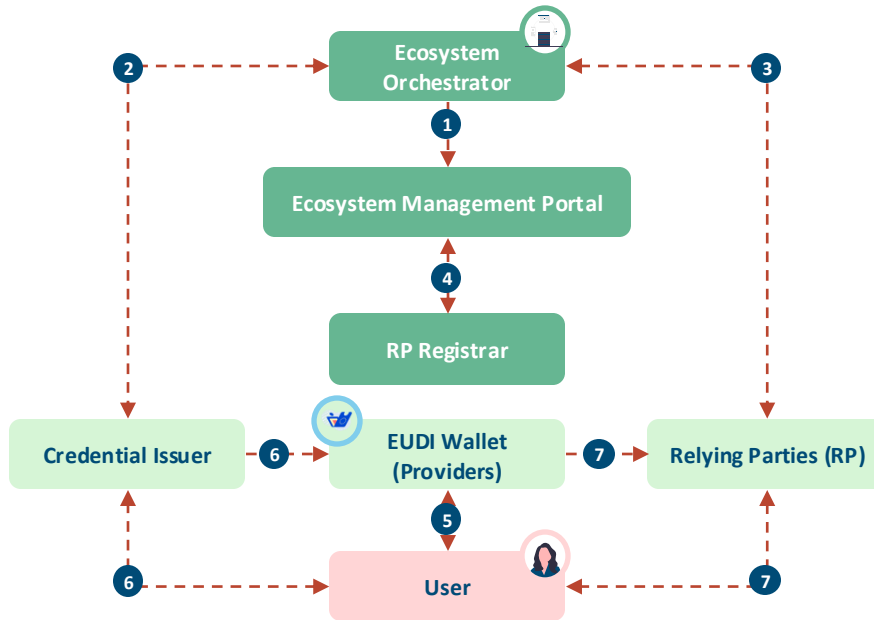
An eudi wallet ecosystem management portal is the central hub for ecosystem access and information



EUDI Wallet Ecosystem Management Portal: Target Vision of Seven Core Functions



The ecosystem management portal plays a central role in the rollout of the ecosystem



- 1** The Ecosystem Orchestrator is responsible for the Ecosystem Management Portal and operates it
- 2** All credential issuers, such as driver's license issuers, register and identify themselves in the Management Portal in order to be able to issue credential to the EUDI Wallet
- 3** All relying parties (e.g., banks or public authorities) register and identify themselves in the portal in order to obtain certificates that allow them to retrieve attestations from the EUDI Wallet
- 4** As the central supervisory authority, the RP Registrar can use the portal to check registration and access certificates and revoke them if necessary
- 5** Users select their EUDI Wallet provider, in whose wallet app they wish to store and manage their credentials
- 6** At the user's request, credential issuers issue the desired credentials to the selected wallet, e.g., educational qualifications or a health insurance card
- 7** At the user's request, the EUDI Wallet transfers evidence to relying parties, e.g., personal identification data when opening a bank account

Six design principles shape the development of the ecosystem management portal



Easy target group-specific access & feature upgrades as needed



Transparency & public control through Open Data by Design



Compliance with the emerging eIDAS 2.0 requirements for the EUDI Wallet ecosystem in the form of a user-centric end-to-end solution

Modular design & iterative development based on dynamic requirements



Open Source & reuse options for e.g., other EU member states



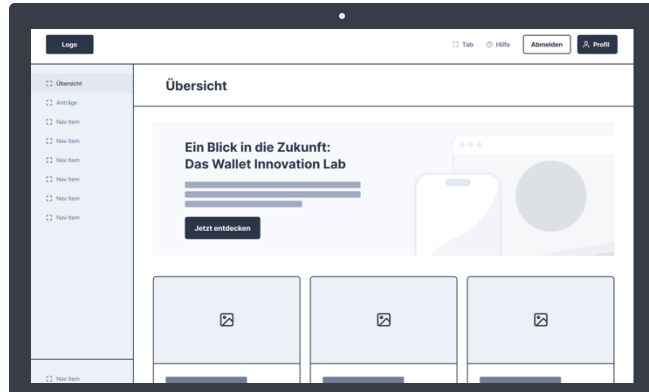
Privacy and security by design, as well as consideration of the requirements of public administration



Users get easy access and organizations manage their interactions in one account



Quick registration with email verification for easy ecosystem access for interested and active members of organizations



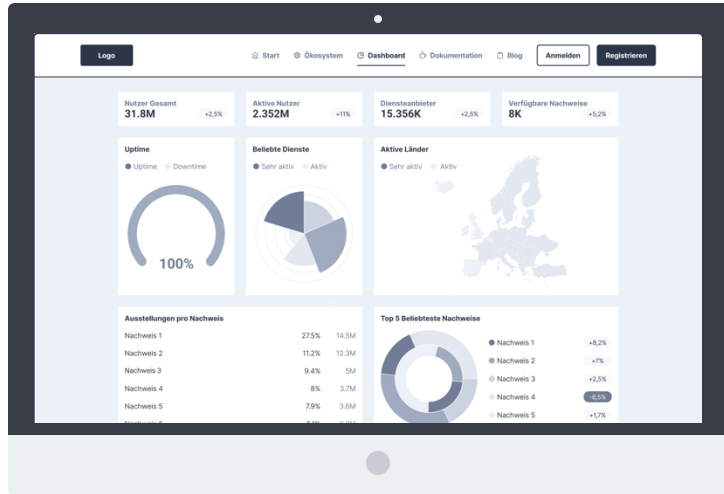
Upgrade to a custom organization account to **manage all features with a single organization dashboard**

All legal, technical, and commercial onboarding steps* are covered in a modular format



**Initial considerations, which may still evolve during development*

All organizational information and key KPIs are published in an ecosystem dashboard



Overview of EUDI Wallet ecosystem KPIs including operational status



Information about organizations and their use cases with the EUDI Wallet will be published



All data is published in machine-readable open data format

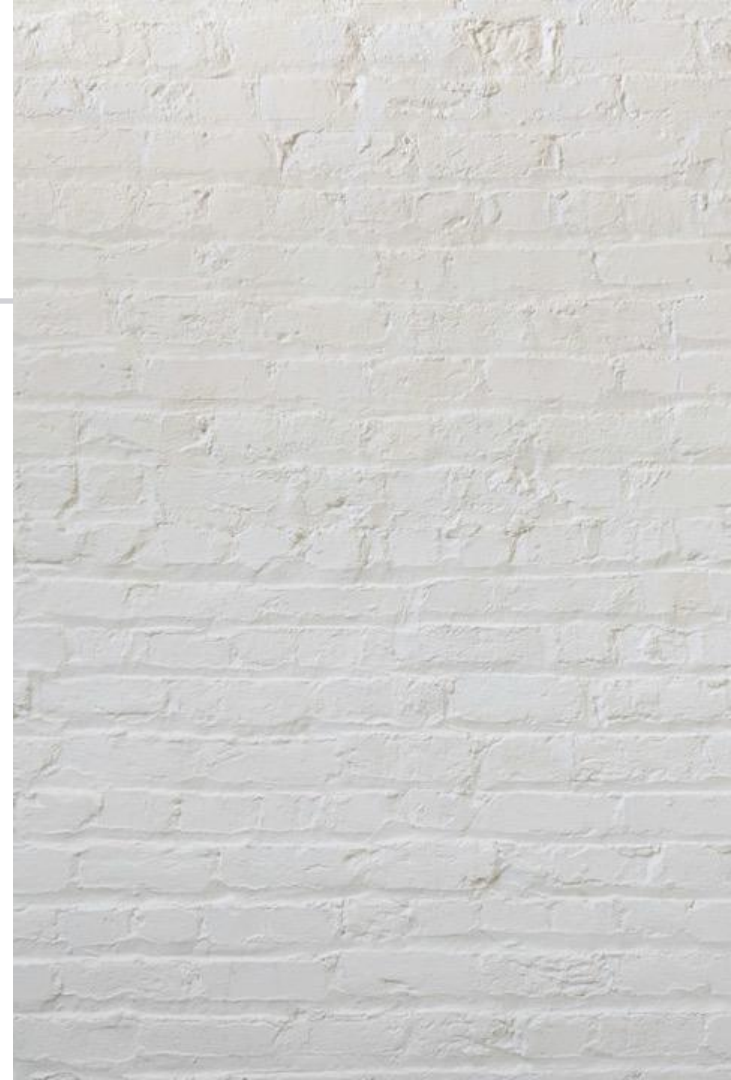


QUALITATIVE INTERVIEWS LEARNINGS END-USERS

THE EUDI WALLET CONSULTATION TEAM

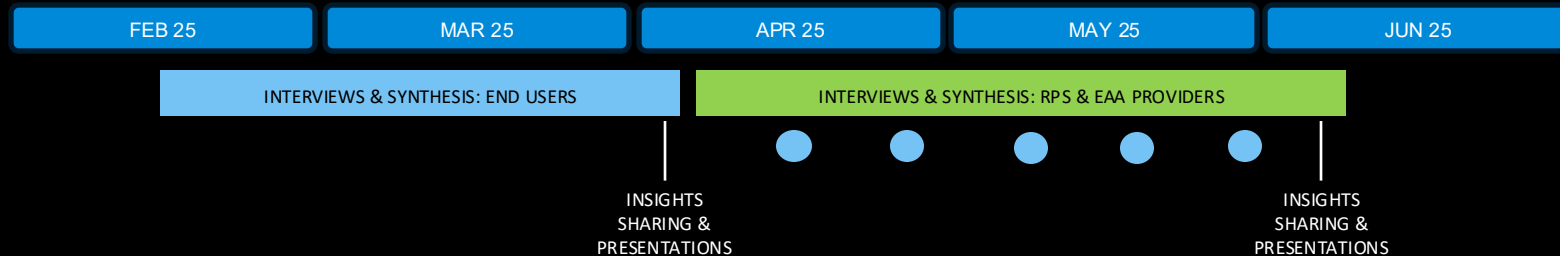
AGENDA

1. Purpose of Today
2. Value Proposition: End Users
3. Research Methodology: Qualitative Interviews
4. Wallet Operator Preferences
5. Interviews with End Users: Insights
6. How does this change the value proposition for end users?



1. END USERS

2. RELYING PARTIES & 3. EAA PROVIDERS (BECAUSE THEY'RE USUALLY BOTH)



VALUE PROPOSITION: END USERS

Value Proposition for Users



Comfort and efficiency

Intuitive and easy to use for all societal user groups



Control over Personal Data

Provide transparency on which data are shared with whom



Enhanced privacy

Support pseudonyms and hinder overidentification



High Level Security

Safeguard personal information from cybercrime and fraud



Better access to Services

Non-discriminatory access to end-to-end digital processes



Legal Recognition

Cross-boarder acceptance of electronic attestations



Free QES for non-professional use

Easily sign documents and confirm data

METHODOLOGY: QUALITATIVE RESEARCH

QUALITATIVE RESEARCH

Interviews are a form of qualitative research. This type of analysis enables us to **understand people deeply** – to identify their **behaviour**, understand their **context**, and understand what **values drive their behaviour**. The sample size is small, but this method is about going deep rather than broad.

Quantitative research is used to size a problem or market, and qualitative research is **used to understand and empathise with people**. Qualitative research is **not representative, nor does it correlate to a place's wider population**.

When possible, qualitative data can be further supported by relevant quantitative data as well as stakeholder information to provide better weighting and information reliability.



WE WON'T...

GIVE PERCENTAGES

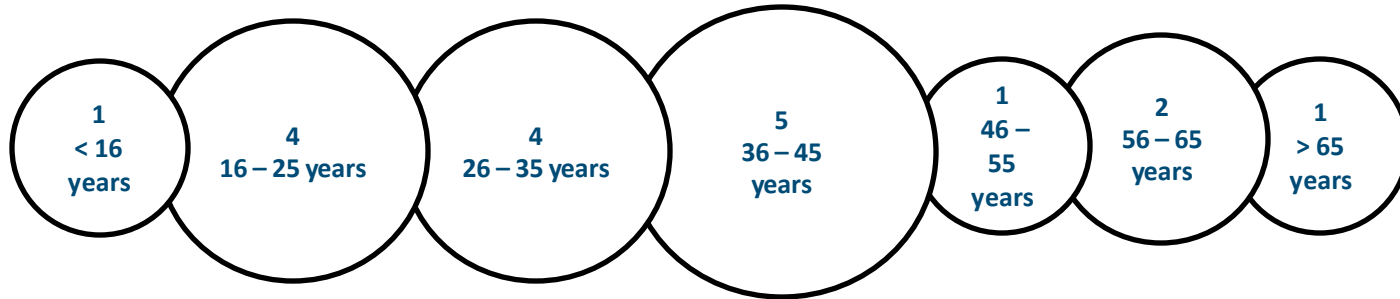
GIVE DEFINITE YES OR NO
CONFIRMATIONS

WE WILL...

PROVIDE LEVERAGE POINTS
AND CAUTION SIGNS
FOR EVIDENCE-BASED DECISION
MAKING

INTERVIEWS WITH END USERS – SAMPLE

18 



7 ♀

11 ♂

Mostly academic background
3 non-academic background
1 high school student
2 retirees

Interviews were completed in person,
online and by telephone from
10th to 23rd of March 2025

WALLET OPERATOR PREFERENCES

A GOVERNMENTAL WALLET

TRUST IN REGULATION BUT AN UNDERLYING MISTRUST IN TECHNICAL CAPABILITY.

For:

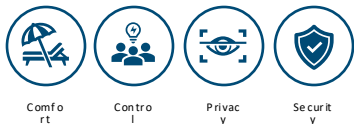
- Not profit driven
- Belief that it's better regulated and protected – trustworthiness
- A German operator in Germany would be more secure

Against:

- Past experience with bad governmental UX and apps
- Belief in a lack of government design and technical competency
- Rise in right wing politics – concerns that data could be misused in a governmental change

CHANCE: Potential to wow the public with good UX and tech!

How might we: ensure this stays cutting edge and up-to-date?



"I'd prefer the governmental wallet - they'd be more trustworthy than Google because no business would be done with data."

"So far, government apps are not convincing. The better programmers are in the private sector."

"I would prefer a government wallet because they are not profit-driven."

"As long as we don't have a far-right, unconstitutional government here, I'm not worried about it."

"I'd want a legal clause that data will not be misused, especially in the event of a change of government."

"I wouldn't say I trust the state per se, but I do trust the laws on data protection issues."

"I have nothing against any start-ups that can make great apps. They can change, are not permanent, are sold, then it goes to someone else. They do it to make money. The state certainly does it too - but it stays. It's stable."

A COMMERCIAL WALLET

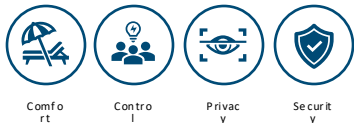
GETTING THE BEST DESIGN AND TECH AT THE POTENTIAL COST OF PERSONAL DATA.

For:

- Belief they are more technically up-to-date and cutting edge
- Belief that they have better security, design and UX
- Integration with existing services – e.g. Google and Apple

Against:

- Profit driven – other agendas
- Data as a business
- Private companies can be bought out by others
- Smaller unknown companies



"From something big" (familiarity) > assume that it works better and is more data-secure > Apple rather than a startup made up of three people; on the other hand, the company may also have more vested interests."

"No no-names - rather something you already know by name - not a start-up from India."

"I think Google is more secure than the state, honestly."

"Never Meta – I would avoid their wallet as I'm very against them."

"I don't trust the government – the technology behind it is crucial. I trust Apple more than the government."

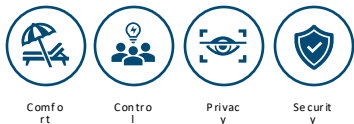
"Providers should not be able to make money from our data."

"So far, government apps are not convincing. The better programmers are in the private sector."

DISTRUST FOR CERTAIN WALLET OPERATORS EVEN THOUGH ALL MUST FOLLOW THE SAME REQUIREMENTS.

- Some preference for a **neutral operator**, non-governmental and non-profit, such as an **official institution**
- More trust in the security of a **domestic operator**
- **Public private partnerships** can ensure the best of all worlds
- Expectations for **easy transfer between different wallets** – no feeling of being locked in and dependent on one operator

There is clearly no one-size-fits-all solution when it comes to wallet operator preferences. This reinforces the necessity to offer the option of multiple operators – but can there be too many?



"Would like a non-governmental and non-profit organization to make it generally a neutral provider."

"I'd find it good to have a combination of them all."

"I have no criteria that exclude certain operators. It should be a domestic company."

"I would have confidence if it was from an 'official institution' e.g. a university."

"It would be very important to me that the German wallet would be operated by a German operator and that the entire infrastructure would also be located here. By that I don't just mean the official postal address."

"A good wallet is enough, plurality is still good, but jungle is unfavorable > no longer clear what is verified and what to look for in the app store."

INTERVIEWS WITH END USERS

INSIGHTS OVERVIEW

01: Comfort and efficiency outweigh concerns.

02: The EUDI wallet offers simple value to the less digitally savvy.

03: Longer setup for EUDI-wallet creates the perception of better long-term efficiency and security.

04: Digital must be simpler than analog alternatives

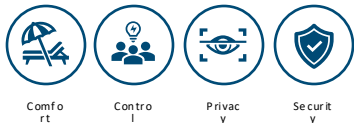
05: People feel powerless against data theft and security breaches.

06: End-users expect transparent continuous development.

07: For many, the real issue is the hassle of recovering from Identity theft and loss, not the theft itself.

08: Past experiences deeply shape mistrust. Without negative experiences, end-users behave naively.

09: There are individually different assessments of which data make up your personal identity and how it should be protected.



01: COMFORT AND EFFICIENCY OUTWEIGH CONCERNS.

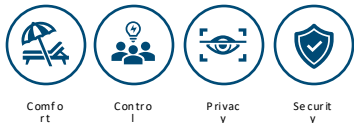
We believe this means...

That **most people prioritise good useability, convenience, comfort and efficiency over data protection, security, and privacy** – whether they voluntarily admit it or are aware of it.

Despite claiming how important they value data security and privacy; they conduct actions that contradict this **due to impatience or frustration**. Sometimes, they need or want a service enough that it **warrants a slip in their otherwise 'secure behaviour'**.

More benefit = more tolerance for less security.

What are your thoughts?



"If I have to use an app that is super secure but barely usable because the developers haven't done their homework, then I won't use such an app."

"I'd rather have a simple app than data protection, because they can see me through the camera anyway."

"Data security and data protection are requirements that I take for granted - everyone is committed to security and data protection, and nobody will voluntarily admit that security is not good because other things take priority."

"A good interface and a good UI make up half of the app."

"It should be fun. I would put the fun of using the app before data protection."

"I'm not a patient person. Either the app is good, i.e. easy to use and does what it's supposed to do, or I don't use it. This applies to both apps and digital services."

"I interact with these entities because I want something from them (a banking service or a hotel room) and if I refuse to share certain data, then I won't get that service. So I will accept. "

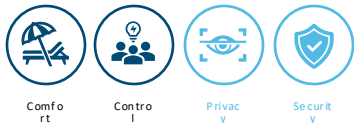
02: THE EUDI WALLET OFFERS SIMPLE VALUE TO THE LESS DIGITALLY SAVVY.

We believe this means...

Having all their **documents digitally accessible in one place and using it in an analogue way** (i.e. physically showing the screen) is the added value that many see as **relevant on a daily basis** – particularly the elderly, the less technical, and frequent travelers.

However, a lot of people are still **not willing to completely rely on digital** and will **bring physical printouts** with them as a form of back up. It's still not rooted enough in their daily lives to do things digitally.

What are your thoughts?



"Registration certificate - I find the idea of having this information digitally in one place very satisfying and clear. It gives me control."

"It would be great if the wallet also offered space for other documents - such as library cards. To really be an alternative to a normal wallet."

"It's useful but possibly when traveling with children: having everything with her in one place (more convenient and easier). On the other hand, I wouldn't leave everything at home because of this - perhaps linking a variant with the partner as a backup would be useful."

"Yes, a convenient solution. Nevertheless, I always print everything out beforehand to avoid any nasty surprises at the counter. Especially when I'm travelling for a long time."

"Control for me is having an overview and understanding - when everything is in one place and I can check it anytime, e.g. when something needs to be renewed."

"I like the fact that I don't have to carry everything with me. If I just sit at home and don't travel, then it's no use to me."

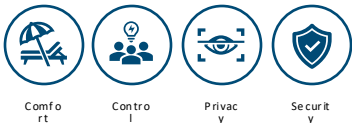
03: LONGER SETUP FOR EUDI-WALLET CREATES THE PERCEPTION OF BETTER LONG-TERM EFFICIENCY AND SECURITY.

We believe this means...

Many expressed a certain level of **tolerance and understanding** if the EUDI-Wallet would require a **longer setup and onboarding processes**.

They seemed to associate the idea that the **extra time and effort spent in the setup correlates to more efficiency and security in the long term**. The question is, how much more time and effort is allowed to still be acceptable and even seen as advantageous?

What are your thoughts?



"I can imagine that loading all the documents into the wallet must take a little longer than using the wallet later. But as soon as I have all the documents in there, it should be quick."

"Time required for setup is acceptable if easier in the long term."

"I can live with one more click if the app fulfils these two requirements (data security and protection)."

"Initial installation and setup must be simple – it may take longer but it should be understandable and have a good overview."

04: DIGITAL MUST BE SIMPLER THAN ANALOG ALTERNATIVES

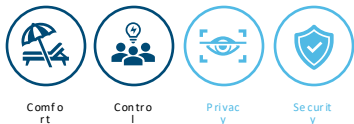
We believe this means...

There is **no tolerance** for digital to be **more cumbersome than existing analogue alternatives**. The expectation is that this will enhance ease-of-use and simplify processes – not complicate.

This is especially important in the analogue use of the EUDI-Wallet where any form of identity **needs to be quick and easy to retrieve**.

Physical breaks in the digital process, such as waiting for an activation letter by mail tend to also **leave a bad aftertaste**.

What are your thoughts?



"To really be an alternative to a normal wallet. However, the app would have to be well thought out if you were to store any certificates, proof of identity, etc. there. Everything I need in my everyday life must be quick and easy to find."

"It was feasible, but I had to wait for a letter."

"I have to turn the thing on and know where my ID is, where my certificate is, where my BahnCard is and not have to click five times or call the hotline to find out which click sequence I have to use."

"Don't want to wait until I receive an email or message with a code that I have to enter before my ID card can be read, for example."

"A digital solution should not be more complicated than its analogue equivalent. Providing a digital solution just for the sake of digitalisation makes no sense to me. It has to really simplify my everyday life and not frustrate me because I need a lot of steps to perform an action or have to remember for a long time how to perform a certain action."

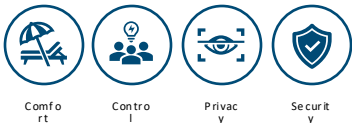
05: PEOPLE FEEL POWERLESS AGAINST DATA THEFT AND SECURITY BREACHES.

We believe this means...

People feel that they're at the **mercy of hackers, data leaks and breaches**. The lack of tangibility makes it hard to see and understand, resulting many to **blindly trust security standards or technologies they do not really understand**. They believe breaches are **inevitable** and it's too late worry about our personal data because it's already being used.

This leads to the choice that they can live in fear and stay behind or use a new service they want and **accept that s**t can happen**. But with the **German EUDI Wallet**, users are **less powerless** and this **needs to be communicated**.

What are your thoughts?



"I'm always very concerned about data theft and fraud and just hope that everything will go well."

"To know that it has good data protection is difficult to assess because it's so hard to see."

"I already use Google so it would work well with all the other Google services. Plus, they have my data anyway."

"You can't see the security. It happens and something WILL happen at some point. We can't prevent everything. We can only try."

"I trust that it works, but I also know that there are ways to steal data. It's like being robbed - it can happen, but the chances are very small."

"I don't want data profiles to be created, but I have the feeling that it can't be avoided."

"No more insecure than physical goods."

"If someone can do mischief with something, then they will find their way."

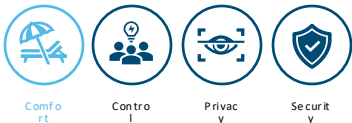
06: END-USERS EXPECT TRANSPARENT CONTINUOUS DEVELOPMENT.

We believe this means...

Many people **understand** hackers, methods and technologies evolve and improve. They **expect that the EUDI Wallet also does the same.**

We need to **prove and communicate that today and in the future the German EUDI Wallet will be cutting edge** – which can **impact adoption and usage**. There needs to be a reaction to end users' complaints and a continuous improvement of the wallet.

What are your thoughts?



"Test, test and test. And from different places. It's better to know where you have a vulnerability and remove it, rather than pretending you've done everything perfectly from the start. The world is evolving every day. This also applies to cybercrime."

"Transparent display of which data is shared. Possibility to confirm data release manually."

"There is no such thing as certainty when it comes to security - security is only a snapshot in time and can change from one day to the next."

"It's like that now, it was like that 50 years ago, it was like that 100 years ago. Only now it's on a different level. They (fraudsters and hackers) will always find holes where they can strike."

"I just want to get warnings that something has happened, that you can react to it. Then I expect the app to take action to prevent further damage."

"I really appreciate it when someone has the courage to say what is currently not sufficiently secure. That allows you to deal with the situation. Trust comes from honesty, not from big promises."

07: FOR MANY, THE REAL ISSUE IS THE HASSLE OF RECOVERING FROM IDENTITY THEFT AND LOSS, NOT THE THEFT ITSELF.

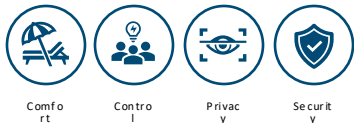
We believe this means...

Some are more concerned about the **inconvenience and the loss of access** they would have to **everyday services that make their lives easier**.

They are more deterred by the **complicated process and time-consuming bureaucracy** to regain and restore access than they are of somebody else walking around and taking actions in their name.

There needs to be a **kill switch** so that nothing can happen, but also a **quick and simple way to recover everything** for user.

What are your thoughts?



"I'm afraid that when it's all gone, I'll have to set everything up again. Restoring should be easy. That everything is restored."

"I'm really scared of having my mobile phone stolen. Not afraid that someone will steal my data, but because I'm completely out of the loop."

"If this added value is stolen from me, then I can't use it. (people + account data), it is also time-consuming to apply for everything again."

"I don't want all my data to be gone or accessible in the event of a data leak."

"Loss scenario important, quick blocking option (kill switch)."

08: PAST EXPERIENCES DEEPLY SHAPE MISTRUST. WITHOUT NEGATIVE EXPERIENCES, END-USERS BEHAVE NAIVELY.

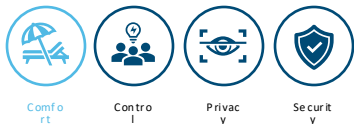
We believe this means...

Those who know someone or had **personally experienced** identity theft, data leaks or being surveilled were **more skeptical** about security systems and **careful** with their online actions.

Conversely, those without such experiences are **more willing to take their chances** and **try new services**.

Making people aware of identity and data theft should be part of a future communication campaign.

What are your thoughts?



"Who would identity theft happen to?"

"I think Google is more secure than the state honestly – there has never been a hacker in my Google account."

"There is theft and there is hacking, but being affected by it is more of a minor occurrence, and my data is safe in one place, such as payment apps."

"It's (identity theft and data leaks) never happened to me before."

"Media and above all personal experience with the StaSi. Also concerned that the state will take advantage – also, relatives have experienced phishing scams."

"No real concerns due to a lack of bad experiences."

"I share my ID and banking card via WhatsApp and E-Mail."

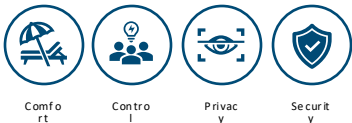
09: THERE ARE INDIVIDUALLY DIFFERENT ASSESSMENTS OF WHICH DATA MAKE UP YOUR PERSONAL IDENTITY AND HOW IT SHOULD BE PROTECTED.

We believe this means...

There is **mixed understanding and value** regarding what data makes up each person's individual identity and is worth protecting. Essentially the most sensitive data is what people **identify their lifestyle** with and **can be used to create a profile, cause inconvenience or lead to discrimination and stalking.**

This has an impact on selective disclosure and influences the need for customization. It would be interesting if users could decide if they could put certain data on higher protection.

What are your thoughts?



"There's no data worthy of protection, since the master data is always freely available somehow and somewhere."

"I have a passport under any government, this is not sensitive data."

"There are different types of data - most of the data that I get taken from me is not data that I worry much about getting out - except maybe phone number and email, where I might get a lot of spam."

"I have nothing to hide - what should they do with it. Only criminals have something to hide."

"Most likely health data, e.g. health card and a combination of various data is rather sceptical (profile, account data). But I would also not rule out storing this type of data in the wallet."

"The wallet should not be possible to browse through my health records or call up my account balance. There should also be no internal connection to the data of my children or my husband."

"My address is especially worthy of protection."

"Under no circumstances GPS tracking => movement profile."

"Loan agreements employment contract birth certificates / general documents (stored in the cupboard at home and partly in the cloud) bank account and information."

HOW DOES THIS CHANGE
THE VALUE PROPOSITION
FOR END-USERS?

Value Proposition for Users (before)



Comfort and efficiency

Intuitive and easy to use for all societal user groups



Control over Personal Data

Provide transparency on which data are shared with whom



Enhanced privacy

Support pseudonyms and hinder overidentification



High Level Security

Safeguard personal information from cybercrime and fraud



Better access to Services

Non-discriminatory access to end-to-end digital processes



Legal Recognition

Cross-boarder acceptance of electronic attestations



Free QES for non-professional use

Easily sign documents and confirm data

Value Proposition for Users (Now)



Comfort, Convenience and Efficiency

Intuitive and easy to use for all societal user groups



Trust in High Level Security

Safeguard personal information from cybercrime and fraud



Control over Personal Data

Provide transparency on which data are shared with whom



Enhanced Privacy

Support pseudonyms and hinder overidentification



Better Access to Services

Non-discriminatory access to end-to-end digital processes



Legal Recognition

Cross-boarder acceptance of electronic attestations



Free QES for non-professional use

Easily sign documents and confirm data

Thank you for your attention!

Contact:

Kristina Yasuda

Federal Agency for Breakthrough
Innovation

E-Mail: kristina.yasuda@eudi.sprind.org

Questions & Answers