

"Irresponsible and dangerous"

The ID wallet for the digital driver's license is not only technically immature. Government disclosures show: The allocation was non-transparent, security checks were incomplete - and the potential targeting is questionable.

The ID Wallet for the digital driver's license had a digital accident: One week before the federal election, it was presented to the public by Transport Minister Andreas Scheuer (CSU), barely a week later it had already disappeared from the Apple and Google app stores.

This was partly due to security concerns expressed by members of the Chaos Computer Club (CCC): On the one hand, attackers could have verifiably taken over a subdomain of the ID Wallet operator and thus impersonated it. This would have resulted in further attack and threat scenarios, says the security expert, who analyzed the app together with Lilith Wittmann. The problems pointed to "weak system administration."

On the other hand, data and identity theft was possible under certain circumstances, as Lilith Wittman describes. That didn't apply to driver's license checks, however, but only to other use scenarios for ID Wallet, such as digital check-in at a hotel.

Still, that - along with an overload problem - was enough to temporarily take the app off the market, even if the still-incumbent federal government initially wanted to start small. For now, it wanted to use the digital driver's license stored in the ID Wallet to make it easier to rent cars or use car-sharing services. In the long term, the digital image of the driver's license on the smartphone should be able to completely replace analog ID documents. The Minister of State for Digitalization, Dorothee Bär (CSU), was the main advocate of this.

"Maximum intransparency"

For Anke Domscheit-Berg, network policy spokesperson for the Left Party's parliamentary group in the Bundestag, the issue is far from over with the announced improvements. "This is not just a temporary setback and another isolated example of a failed project in digitization," she tells SPIEGEL. Rather, she says, the German government has "massively gambled away" the trust of the population that is necessary for such projects. She is not only concerned about the inadequate IT security of the ID Wallet, but also about the government's awarding practices and the future organization of the project.

Domscheit-Berg had asked the German government several written questions about this. Dorothee Bär's answers, which have not yet been published, have been made available to SPIEGEL, and Domscheit-Berg considers them alarming.

When asked, for example, how many providers applied in the tender for the ID Wallet project, Bär replied that there had been no tender. She put it this way: The federal government had decided to use an existing framework agreement with System Vertrieb Alexander GmbH (SVA), "in which IBM Deutschland GmbH as well as Esatus AG are subcontractors in the project. "As a subsidiary of Esatus AG, Digital Enabling GmbH is the publisher of the ID Wallet developed by Esatus AG." Domscheit-Berg considers the practice of making a "completely unknown" subsidiary of a subcontractor the publisher to be "intransparent to the maximum."

She is also surprised by the company's possible future role. For Bär wrote: "Talks are currently underway between BReg (the German government - editor's note) and the companies involved in the overall project about permanent governance for the overall digital identities ecosystem." To this end, "the establishment of a public-private joint venture is being considered, which would be owned 50 percent each by the public sector on the one hand and the private sector on the other, and would assume operational responsibility for the ecosystem."

Domscheit-Berg considers the contemplated establishment of such a public-private partnership (PPP) "a serious mistake." Because in PPP companies, "risks are often distributed one-sidedly to the public partner and profits one-sidedly to the private partner," and in addition, "there is almost

always a lack of sufficient control options and sufficient transparency, the consequences of which we know from expensive loss-making transactions such as Toll Collect."

For the MEP, one thing is certain: "Verified driver's license data or comparable data from state documents should be treated like sovereign documents, they do not belong in the control of private companies in which the state does not even hold shares." Translated with www.DeepL.com/Translator (free version)

"No consideration or review of the specific implementation".

Domscheit-Berg also wanted to know whether the German Federal Office for Information Security (BSI) and the Federal Data Protection Commissioner had reviewed the app before it was published. Bär's answer: the BSI had only reviewed another use case of ID Wallet, the digital hotel check-in. "In this context, numerous improvements were implemented," it says. "In addition, necessary further development needs for the system concept were identified before the pilot application goes into open active operation. This is being worked on."

Regarding the digital driver's license, the authority had only been provided with the documentation and "explained in several rounds of questions." The BSI, however, "did not carry out any examination or review of the actual implementation, as it was not called upon to do so due to its responsibility."

The Federal Data Protection Commissioner, in turn, advises the federal government on the overarching "secure digital identities" project. But he offered "no testing or certification of isolated apps, especially not from private publishers."