Passkeys –

a sophisticated alternative to passwords

Ulrich Jetzek
Faculty of Computer Science and
Electrical Engineering
Kiel University of Applied Sciences
Kiel, Germany
Ulrich.Jetzek@fh-kiel.de

***Abstract*— In today's world with an uncounted number of applications and services being used by a countless number of users fast, reliable and even more important: secure authentication of users is crucial for individuals, organizations and companies around the world. While the combination of user name and password was common for long time in many systems, due to phishing and other attacks more secure authentication methods are needed. Passkeys are a promising and strong alternative to passwords. This paper will give insight into the idea and priniciples for passkeys. In addition it will address the benefits that passkeys provide as compared to conventional passwords.**

In the first section we will address passwords from a cryptographic perspective: Passwords correspond to a symmetric crypto system, where the secret password must only be known by the user and the corresponding application server. We will see that passwords have quite some disadvantages. Apart from the possibilities of guessing simple passwords users may apply (e.g. summer25), passwords are subject to phishing and other attacks.

Therefore, more sophisticated methods for user authentication are needed for today's applications and services. At this point the FIDO organization [1] and passkeys come into the game [2]. The idea of passkeys is based on the principle of asymmetric crypto systems. For such systems the smartphone or laptop user creates a key pair that consists of a public key and a private key. The public key will be sent to the application server and allows anyone to encrypt a specific plain text message. However, due to the fact, that the creation of the above mentioned key pair makes use of so called trapdoor or one-way-functions, decryption of an encrypted message is only possible by using the private key. Therefore, only the smartphone or laptop user may decrypt a specific encrypted message. This idea will be described in this paper by using the RSA crypto system [3]. Within the presentation it will be shown, that RSA is based on the socalled integer factorization problem. RSA requires the exponentiation of an integer x, the plain text, with the public exponent e modulo a large composite number n, where n is the product of two large primes p and q. Although it is not possible to factorize n into its prime factors p and q for any third party, it is possible for the smartphone user to calculate Euler's Phi-function $\Phi(n) = (p-1)\cdot(q-1)$. By doing so, it is possible for the user to compute the multiplicate inverse $d = e^{-1} \; mod \; \Phi(n)$, which is needed to compute the plain text x out of an encrypted cipher text $y = x^e \; mod \; n$. Within this paper we will also show a simple cryptographic protocol based on RSA which may be used for secure user authentication. This protocol contains the advantage, that no secret password or the like needs to be stored on the application server, nor does the system suffer from possibly 'simple' passwords. Passkeys and the used protocols are always strong and are phishing resistant. Therefore passkeys will receive more attention and will most likely be the authentication method for many – possibly all – future applications and services.

Keywords*— *passwords, passkeys, FIDO, symmetric cryptography, asymmetric cryptography, RSA, integer factorization problem, Euler's Phi-function

I. LITERATURVERZEICHNIS

[1] wikipedia, „FIDO-Allianz," 01 September 2025. [Online]. Available: https://de.wikipedia.org/wiki/FIDO-Allianz .

[2] FIDO Alliance, „passkey central," [Online]. Available: https://www.passkeycentral.org/home. [Zugriff am 01 09 2025].

[3] C. Paar und J. Pelzl, Understanding Cryptography, Heidelberg: Springer Verlag, 2010.