Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V.
Bundesverband deutscher Banken e. V.
Bundesverband Öffentlicher Banken Deutschlands e. V.
Deutscher Sparkassen- und Giroverband e. V.
Verband deutscher Pfandbriefbanken e. V.

Die Deutsche Kreditwirtschaft

German Banking Industry

FIDO2: proposed amendment for the secure display of transaction data

Lobby Register No R001459
EU Transparency Register No 52646912360-95

Contact:
Diana Campar
Associate Director
Telephone: +49 30 1663- 1546
E-Mail: diana.campar@bdb.de

Berlin, 20 March 2025

The **German Banking Industry Committee** is the joint committee operated by the central associations of the German banking industry. These associations are the Bundesverband der Deutschen Volksbanken und Raiffeisenbanken (BVR), for the cooperative banks, the Bundesverband deutscher Banken (BdB), for the private commercial banks, the Bundesverband Öffentlicher Banken Deutschlands (VÖB), for the public banks, the Deutscher Sparkassen- und Giroverband (DSGV),
for the savings banks finance group, and the Verband deutscher Pfandbriefbanken (vdp), for the Pfandbrief banks. Collectively, they represent approximately 1,700 banks.

Coordinator:
Bundesverband deutscher Banken e.V.
Burgstraße 28 | 10178 Berlin | Germany
Telephone: +49 30 1663-0
www.die-deutsche-kreditwirtschaft.de
www.german-banking-industry.org

FIDO2: proposed amendment for the secure display of transaction data

German Banking Industry Committee recommendation on amending FIDO2

The German Banking Industry Committee (GBIC) believes that the FIDO standard represents an important foundation for a secure, sustainable, effective and highly convenient authentication method. The standard currently focuses largely on logging in to platforms and systems. GBIC, however, is calling for the standard to be expanded to include transactions and business activities (referred to as "transactions" below) carried out on these platforms. For the banking industry, this primarily refers to online banking and card payments.

Secure, dynamic confirmation of transactions is a major requirement for strong customer authentication processes in online banking. The German Banking Industry Committee, an alliance of German banking associations, evaluates existing and new authentication procedures in regard to their security features and compliance with regulations, in particular as pertaining to compliance with current requirements from the revised Payment Services Directive (PSD2) and forthcoming requirements from the Payment Services Regulation (PSR).

FIDO2 offers a standardised solution for two-factor authentication using a hardware token, implemented using WebAuthn and CTAP. Unfortunately, the Client to Authenticator Protocol (CTAP) does not currently support the secure display of transaction data via the hardware token (authenticator); the German Banking Industry Committee, however, believes that this is an essential requirement for facilitating dynamic confirmation of transactions and ensuring they cannot be manipulated.

Essential: secure display of transaction data

The PSD2 and the associated delegated regulation (RTS) require that transaction data be displayed authentically as an integral element of secure transaction authentication. Currently, the FIDO2 CTAP only provides for transmission of a hash value representing the transaction data to the authenticator, but not the actual transaction details. This means that the client would have to confirm the current transaction without being able to view its details directly on the authenticator.

This limitation is a particular and significant security risk in combination with PC architecture, which cannot guarantee a secure runtime environment. Malware could manipulate transaction data without a client's knowledge. Transaction data displayed authentically on a separate hardware token is therefore imperative in order to prevent this from happening.

FIDO2: proposed amendment for the secure display of transaction data

Recommendation: amend FIDO2

Given the issues explained above, the German Banking Industry Committee recommends that CTAP be expanded to include a feature allowing for the secure display of transaction data, which could be achieved as follows:

- **Transmit transaction data to the authenticator:** instead of sending only a hash value, the full transaction data should be transmitted to the external authenticator.
- **Integrate a secure display:** authenticators with displays should be expanded to show users the transmitted transaction data, which the user can then verify.
- **Link the authentication code to the data on display:** the authentication code generated by the authenticator should include a hash value which is calculated by the authenticator for the data shown on the display, so that the authentication code is securely linked to this data. This will allow the bank to verify the secure display and confirmation of the transaction data.
- **Expand the CTAP specification:** The FIDO Alliance should expand CTAP to include a standardised interface for transmitting and displaying transaction data.

In our opinion, the current FIDO2 implementation does not yet fulfil the regulatory requirements for a secure display of transaction data, and therefore cannot be used for secure authentication in online banking. We therefore strongly recommend amending CTAP in order to guarantee security and integrity for transaction confirmations. This amendment would not just allow FIDO2 standards to be implemented in the financial sector, it would also increase user confidence in FIDO2-based authentication methods.