One-Time-Passcode (OTP) Display Card

Definition/Description

An OTP display card is a token in credit card format with a display, an on-off button, and a PIN pad (optional). The card generates a one-time passcode that is used to authenticate the cardholder attempting to access a specific resource or sign a transaction. The PIN pad protects access to the OTP and enables transactions to be signed. If the OTP display card is an EMV chip card, the card can act as a both the Chip Authentication Program (CAP) reader[1] and the payment card.

An OTP display card is an alternative form factor to other OTP generating tokens (e.g., dongles).

Applicability

Channel	Applicable?	Use Case	Applicable?	Stakeholder	Applicable?
In-app [merchant app]	Yes	Customer onboarding	NA	Merchants	NA
Mobile browser	Yes	Authentication (onboarding)	Yes	Issuers	Yes: internal
Desktop/laptop computer	Yes	Authentication (transaction)	Yes	Issuer processors	NA
Phone	Yes	Authorization	NA	Wallet/online payment providers	NA
		Post-authorization review	NA	Acquirer processors	NA

Technical Features/How the Technique Works

When a website asks for entry of a one-time passcode, the cardholder presses the on/off button on the card, enters a PIN if requested, and then enters the code displayed on the card on the website. The server associated with the OTP solution will determine whether the code is correct and allow or not allow login. When using the card to sign a transaction, a challenge-response algorithm is used with a dialogue between the cardholder and the card.

Risks Associated with Technique

The OTP display card has a shelf life based on the presence of a battery on the card. Depending on the type of algorithm used (time-based, or event-based) the card life will vary. The card issuer needs to issue a new card before the battery fails to prevent the cardholder from not being able to use the card for login.

[1] A handheld device that accepts a chip card and has a keypad and display. The CAP reader is used to provide second factor of authentication for CNP transactions. Additional information can found at https://en.wikipedia.org/wiki/Chip_Authentication_Program.

The strength of the technique depends on the cryptography used. This technique is vulnerable to a 'man in the middle' attack.

Customer Impact/Level of Friction

The card form factor provides advantages to cardholders since cards can be carried in a wallet. However, in the case of cards with PIN pads, some users with large fingers may experience difficulty pressing the appropriate keys.

Implementation Considerations

The card issuer needs to have a matching server to authenticate the OTPs generated by the card. The server can be offered as a cloud service.

OTP display cards are more expensive than other OTP devices (such as traditional dongles or clamshell tokens); however, they provide more convenience for the cardholder.

Maturity

The OTP display card is a mature technology.

Applicable Industry Standards

OTP algorithm specifications are either open (e.g., OATH) or proprietary to a vendor.

Publicly Available Statistics on Implementations and Use

Statistics are not available for this technique.

Further Reading

https://openauthentication.org

https://blog.bluepay.com/dynamic-cvv-solution-comparisons

Source Document: This technique is extracted from the *Card-Not-Present (CNP) Fraud Mitigation Techniques* white paper. That white paper was developed to provide a high-level document that directs readers to relevant fraud mitigation techniques while providing easy access to details about the solutions. The white paper is available at: https://www.uspaymentsforum.org/card-not-present-cnp-fraud-mitigation-techniques/

Please note: *The information and materials contained in this document ("Information") is provided solely for convenience and does not constitute legal or technical advice. All representations or warranties, express or implied, are expressly disclaimed, including without limitation, implied warranties of merchantability or fitness for a particular purpose and all warranties regarding accuracy, completeness, adequacy, results, title and non-infringement. All Information is limited to the scenarios, stakeholders and other matters specified, and should be considered in light of applicable laws, regulations, industry rules and requirements, facts, circumstances and other relevant factors. None of the Information should be interpreted or construed to require or promote the establishment of any solution, practice, configuration, rule, requirement or specification inconsistent with applicable legal requirements, any of* *which requirements may change over time. The U.S. Payments Forum assumes no responsibility to support, maintain or update the Information, regardless of any such change. Use of or reliance on the Information is at the user's sole risk, and users are strongly encouraged to consult with their respective payment networks, acquirers, processors, vendors and appropriately qualified technical and legal experts prior to all implementation decisions.*