PASCAL Journal of Computer Science and Informatics
https://jurnal.devitara.or.id/index.php/komputer
E-ISSN: 3047-5074 Volume 1 Nomor 1 Tahun 2023

Implementation of Email-Based One-Time Password Authentication for Securing Student Portal Login

Alwin Fau
Universitas Budi Darma, Medan, Indonesia

ARTICLE INFO

Keywords:
one-time password;
student portal;
authentication;
email OTP;
login security

ABSTRACT

Password-only authentication exposes web portals to risks associated with credential theft, reuse, and guessing. This study implements an email-based One-Time Password (OTP) as an additional verification step for the student portal of Universitas Budi Darma. The prototype generates a temporary token after successful username-and-password verification, sends the token to the registered email address, stores the verification value on the server, and limits its validity to six minutes. The study evaluates the design through functional authentication scenarios and a security-oriented analysis of single use, expiration, credential theft, brute-force exposure, phishing, and transport protection. The implementation adds a second verification step so that possession of a static password alone is insufficient to complete login. However, the analysis also shows that OTP security depends on short validity, attempt limiting, secure transport, protected email access, and safe token generation. The original prototype uses an MD5-derived value; this is retained only as part of the implemented design and is not recommended for production deployment. Standards-based HOTP/TOTP with HMAC-SHA-256 or equivalent modern mechanisms are preferable for future development.

Email:
alwinfau@gmail.com

Copyright © 2023 PASCAL.
All rights reserved is Licensed under a Creative Commons Attribution- NonCommercial 4.0 International License (CC BY-NC 4.0)

INTRODUCTION

Student portals provide access to academic records, schedules, administrative services, and other information that may contain personal or institutionally sensitive data. Because access is commonly protected by a username and a static password, the authentication layer becomes a critical control point. Passwords remain practical, but they are exposed to risks such as reuse, guessing, credential theft, and phishing, particularly when users employ weak or repeated credentials across services (Bonneau et al., 2012; Ometov et al., 2018).

One-Time Password (OTP) authentication adds a temporary credential that is valid for one authentication event or for a short period. Standardized OTP mechanisms include HMAC-based One-Time Password (HOTP), which uses a shared secret and a counter, and Time-Based One-Time Password (TOTP), which replaces the counter with a time-derived moving factor (M'Raihi et al., 2005; M'Raihi et al., 2011). In practice, OTP can be delivered or generated through several channels, including hardware tokens, authenticator applications, SMS, and email. The additional verification step can reduce the impact of a stolen static password, although its security depends on implementation details and the protection of the delivery channel (Grassi et al., 2020).

Previous studies have applied OTP to academic information systems and web login protection. Santoso et al. (2013) implemented an SMS-based OTP for an academic information system using an MD5-derived value, while Azhar et al. (2020) described email-based OTP delivery with a six-minute validity period. Other work has examined TOTP for student attendance, multi-factor authentication for connected devices, and OTP combined with additional authentication factors (Sari & Abdillah, 2021; Chan et al., 2021; Tok et al., 2021). These studies indicate that OTP is useful as an additional authentication layer, but they also show that the protection provided by OTP cannot be separated from token lifetime, channel security, rate limiting, and recovery procedures.

This study implements an email-based OTP mechanism for securing login to the Universitas Budi Darma student portal. The contribution is focused on the authentication workflow and the security implications of a short-lived, single-use token after primary password verification. Unlike claims that OTP alone eliminates phishing, brute-force attacks, or man-in-the-middle attacks, this article evaluates the control more narrowly: OTP reduces dependence on a static password, while secure transport, attempt limiting, and protection of the

registered email account remain necessary. The study also identifies the use of MD5 in the original prototype as a legacy design limitation and discusses a migration path toward standards-based HOTP/TOTP.

METHODS

The research follows a prototype-oriented experimental approach. The object of implementation is the login process of the Universitas Budi Darma student portal. The authentication flow is divided into two stages. In the first stage, the user submits a registered username and password. If the primary credentials are valid, the system creates a temporary OTP and sends it to the email address associated with the account. In the second stage, the user submits the OTP; access is granted only when the submitted value matches the server-side verification value and remains within the validity period.

Authentication Workflow

1. The user enters a username and password on the portal login page.
2. The server validates the primary credentials against the registered account data.
3. After successful primary validation, the prototype derives a temporary OTP value and records the verification value on the server.
4. The OTP is sent to the registered email address as a secondary verification channel.
5. The user enters the received OTP on the verification page.
6. The server checks the submitted OTP, the validity period, and whether the token is still eligible for use.
7. A valid OTP completes authentication; an invalid or expired OTP is rejected.

The prototype uses a six-minute OTP validity period, consistent with the design described in the source report. The short lifetime limits the period in which an intercepted code can be attempted. Nevertheless, token expiration must be combined with server-side attempt limits because a short numeric OTP has a relatively small search space. RFC 4226 explicitly recommends throttling or lockout controls against brute-force attempts (M'Raihi et al., 2005).

OTP Generation and Security Boundary

The original design derives the temporary value using MD5 and stores the corresponding verification value in the database before sending the OTP by email. This mechanism is described here to preserve the implemented research design; it should not be interpreted as a recommendation to use MD5 as a modern cryptographic primitive. For production authentication, standards-based HOTP or TOTP should be preferred because these mechanisms use HMAC with a shared secret, and TOTP permits HMAC-SHA-256 or HMAC-SHA-512 implementations (M'Raihi et al., 2005; M'Raihi et al., 2011).

The security boundary also includes the web session, database, mail delivery path, and the user's email account. OTP does not independently protect a session from a man-in-the-middle attack; transport-layer protection such as TLS is still required. Likewise, an email OTP can be captured if the email account itself is compromised. Therefore, the prototype is evaluated as an additional authentication layer rather than as a complete substitute for secure session management and endpoint protection (Grassi et al., 2020; Ometov et al., 2018).

Evaluation Scenarios

Because the source implementation does not report a large-scale penetration test, the evaluation is limited to functional and design-level security scenarios. The analysis examines whether the authentication workflow enforces the intended control under valid, invalid, expired, and compromised-credential conditions. Claims are therefore restricted to the behavior supported by the prototype design and do not represent a quantified resistance rate against real-world attackers.

Table 1. Functional and Security Evaluation Scenarios

Scenario	Primary Password	OTP Condition	Expected Control
Normal login	Valid	Valid and within 6 minutes	Access is granted after the second verification step.

Incorrect OTP	Valid	Does not match	Authentication is rejected.
Expired OTP	Valid	Older than the validity window	Authentication is rejected and a new OTP is required.
Stolen static password	Compromised	Attacker has no email access	The password alone is insufficient to complete login.
Repeated guessing	Valid	Multiple guesses	Risk remains unless rate limiting / lockout is enforced.
Phishing / real-time relay	Compromised	OTP may also be relayed	Email OTP reduces static-password dependence but is not inherently phishing-resistant.
MITM / transport attack	Any	Any	OTP does not replace TLS; secure transport remains required.

RESULTS AND DISCUSSION

Implementation Result

The implemented workflow adds an email-delivered OTP after successful verification of the username and password. The main functional change is that the static credential pair no longer represents the final authorization condition. A user who knows the account password must also obtain the temporary code delivered to the registered email address. The six-minute validity window provides a bounded period for token use and supports automatic invalidation of old verification values.

From an authentication-design perspective, the additional step improves resistance to attacks that obtain only the static password. If an attacker acquires the username and password but cannot access the registered email account, the login cannot be completed under the intended workflow. This is the principal security benefit supported by the prototype. Similar academic-system implementations have also used OTP after password verification, indicating that OTP can provide a practical second step without requiring dedicated hardware (Santoso et al., 2013; Azhar et al., 2020).

Security Analysis

The security effect of the OTP mechanism should be interpreted according to the threat being considered. For password guessing and credential theft, the OTP creates an additional condition that an attacker must satisfy. However, OTP does not make brute force impossible. A short numeric code remains guessable in principle; the effective defense comes from combining limited validity, single use, and strict attempt throttling. The HOTP specification explicitly treats throttling as a recommended server-side countermeasure, while digital-identity guidance emphasizes lifecycle controls and protection of authenticators (M'Raihi et al., 2005; Grassi et al., 2020).

The same limitation applies to phishing. A conventional OTP can prevent reuse of a previously captured code after it expires or is consumed, but a real-time phishing site may relay a valid OTP during its active period. Therefore, the statement that OTP makes phishing ineffective would be too strong. Research on web authentication and multi-factor authentication shows that security must be evaluated together with deployability, usability, channel compromise, and attacker interaction (Bonneau et al., 2012; Ometov et al., 2018). For a student portal, user education and careful login-page design remain important supporting controls.

Man-in-the-middle protection must also be separated from OTP verification. The OTP confirms possession of the secondary channel at a point in time, but it does not encrypt the communication path. TLS is still needed to protect credentials, OTP submissions, and authenticated sessions while data moves between browser and server. In addition, session identifiers should be regenerated after successful authentication, and the OTP value should be invalidated immediately after successful use to reduce replay opportunities.

Comparison with Standards-Based OTP

Table 2. Prototype Design and Recommended Production Direction

Aspect	Prototype	Recommended Direction
Second step	Email-delivered OTP	Retain as an additional factor when appropriate.

Token generation	MD5-derived value	Use HOTP/TOTP or CSPRNG-generated OTP; prefer HMAC-SHA-256/SHA-512 where supported.
Validity	Six minutes	Use the shortest practical lifetime and invalidate immediately after use.
Guessing control	Not quantitatively reported	Add per-account and per-session attempt limits / throttling.
Transport security	TLS discussed as necessary	Enforce HTTPS/TLS for all authentication and session traffic.
Recovery	Not fully specified	Design recovery so it is not weaker than the primary authentication flow.

Table 2 clarifies that the contribution of the prototype is the two-stage login workflow rather than the continued use of MD5. HOTP and TOTP provide standardized constructions for one-time passwords, and TOTP extends HOTP with a time-based moving factor. Studies from 2021 also demonstrate continued use of OTP in multi-factor systems for attendance, IoT, smart-home, and distributed authentication settings, supporting the relevance of OTP as a deployable secondary mechanism (Sari & Abdillah, 2021; Chan et al., 2021; Tok et al., 2021; Catalfamo et al., 2021).

CONCLUSION

The implementation of an email-based One-Time Password adds a second verification step to the Universitas Budi Darma student portal login process. Under the intended workflow, possession of a static username and password is not sufficient to complete authentication because a temporary code delivered to the registered email address is also required. The six-minute validity period limits the useful lifetime of the code, while single-use verification is intended to reduce replay. The security analysis shows, however, that OTP should not be treated as a standalone defense against all login attacks. Effective deployment also requires attempt throttling, TLS-protected communication, immediate token invalidation, secure email access, and a robust recovery process. The MD5-derived token construction in the original prototype is a legacy limitation; future development should migrate to standards-based HOTP/TOTP or another cryptographically secure OTP generation mechanism. Further work should conduct quantitative penetration testing and usability evaluation on the operational portal.

REFERENCES

M'Raihi, D., Bellare, M., Hoornaert, F., Naccache, D., & Ranen, O. (2005). HOTP: An HMAC-based One-Time Password algorithm (RFC 4226). Internet Engineering Task Force. https://doi.org/10.17487/RFC4226

M'Raihi, D., Machani, S., Pei, M., & Rydell, J. (2011). TOTP: Time-Based One-Time Password algorithm (RFC 6238). Internet Engineering Task Force. https://doi.org/10.17487/RFC6238

Bonneau, J., Herley, C., van Oorschot, P. C., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. 2012 IEEE Symposium on Security and Privacy, 553-567. https://doi.org/10.1109/SP.2012.44

Santoso, K. I., Sediyono, E., & Suhartono. (2013). Studi pengamanan login pada sistem informasi akademik menggunakan otentifikasi One Time Password berbasis SMS dengan Hash MD5. Jurnal Sistem Informasi Bisnis, 3(1), 7-12.

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-Factor Authentication: A survey. Cryptography, 2(1), 1. https://doi.org/10.3390/cryptography2010001

Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Burr, W. E., Richer, J. P., Lefkovitz, N. B., Danker, J. M., Choong, Y.-Y., Greene, K. K., & Theofanos, M. F. (2020). Digital Identity Guidelines: Authentication and Lifecycle Management (NIST SP 800-63B, updates as of 03-02-2020). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63b

Azhar, Arkarni, W., & Atthariq. (2020). Sistem keamanan pada halaman login menggunakan One Time Password. Journal of Embedded Systems, Security and Intelligent Systems, 1(2), 106-113.

Sari, A. N., & Abdillah, T. G. (2021). Metode absensi mahasiswa berbasis QR Code dan Time-Based One-Time Password. Jurnal Informatika Polinema, 7(2), 29-34. https://doi.org/10.33795/jip.v7i2.492

Chan Suet Yan, S., Tang Su Wei, A., Bong, J. H., Teh, Q. L., Sivalingam, S., Khoo, S. Y., & Nafy, T. M. (2021). Authentication of IoT device with the enhancement of One-time Password (OTP). Journal of IT in Asia, 9(1), 29-40. https://doi.org/10.33736/jita.3841.2021

Tok, Y. X., Katuk, N., & Che Mohamed Arif, A. S. (2021). Smart home multi-factor authentication using face recognition and One-Time Password on smartphone. International Journal of Interactive Mobile Technologies, 15(24), 32-48. https://doi.org/10.3991/ijim.v15i24.25393

Catalfamo, A., Ruggeri, A., Celesti, A., Fazio, M., & Villari, M. (2021). A microservices and blockchain based One Time Password (MBB-OTP) protocol for security-enhanced authentication. 2021 IEEE Symposium on Computers and Communications, 1-6. https://doi.org/10.1109/ISCC53001.2021.9631479

Vorakulpipat, C., Pichetjamroen, S., & Rattanalerdnusorn, E. (2021). Usable comprehensive-factor authentication for a secure time attendance system. PeerJ Computer Science, 7, e678. https://doi.org/10.7717/peerj-cs.678