

ABSTRAK

Sistem autentikasi berbasis kata sandi terbukti rentan terhadap berbagai serangan siber seperti *phishing*, *brute force*, dan *credential stuffing*. Kondisi ini semakin kritis dalam konteks digitalisasi layanan publik di Indonesia, termasuk di tingkat kelurahan yang belum memiliki mekanisme autentikasi memadai. Penelitian ini bertujuan merancang dan mengimplementasikan sistem autentikasi *passwordless* berbasis FIDO2/WebAuthn pada prototipe *website* layanan administrasi Kelurahan Karangpucung Purwokerto Selatan, serta menguji fungsionalitas dan keamanannya. Penelitian dibatasi pada implementasi autentikasi FIDO2/WebAuthn mencakup proses registrasi, *login*, dan pemulihan akun menggunakan biometrik sidik jari, dengan fitur layanan administrasi pengajuan Surat Keterangan Tidak Mampu (SKTM) sebagai media pengujian. Sistem dibangun dalam skala prototipe menggunakan data *dummy* tanpa integrasi dengan sistem pemerintah eksternal. Metode yang digunakan adalah *Research and Development* (R&D) dengan model *Prototyping* tiga iterasi. Sistem dikembangkan menggunakan arsitektur *client-server* dengan React.js pada *frontend*, Node.js dan Express.js pada *backend*, MongoDB sebagai basis data, serta *library* SimpleWebAuthn untuk implementasi protokol WebAuthn. Evaluasi penerapan model *prototyping* secara iteratif menunjukkan peningkatan kelayakan sistem, di mana tingkat pencapaian aspek sistem pada evaluasi awal (Iterasi 1) baru terpenuhi 50% (5 dari 10 aspek) dan berhasil meningkat mencapai 100% (seluruh 10 aspek terpenuhi) pada evaluasi akhir (Iterasi 3). Hasil pengujian fungsional menggunakan *Black Box Testing* terhadap sebelas skenario menunjukkan seluruh fitur berfungsi sesuai hasil yang diharapkan. Pengujian keamanan terhadap tiga skenario ancaman, yaitu *phishing*, *replay attack*, dan simulasi *database breach*, membuktikan sistem mampu menahan seluruh ancaman tersebut melalui mekanisme *origin binding*, *challenge* sekali pakai, *counter incrementing*, enkripsi AES-256-CBC, dan peniadaan kata sandi sepenuhnya dari sistem.

Kata kunci: FIDO2, WebAuthn, Autentikasi *Passwordless*, Keamanan sistem, Layanan administrasi kelurahan

ABSTRACT

Password-based authentication systems have proven vulnerable to various cyber attacks such as phishing, brute force, and credential stuffing. This condition is increasingly critical in the context of digitalization of public services in Indonesia, including at the kelurahan level which does not yet have adequate authentication mechanisms. This research aims to design and implement a passwordless authentication system based on FIDO2/WebAuthn on a prototype of the administrative service website of Kelurahan Karangpucung Purwokerto Selatan, and to test its functionality and security. The research is limited to the implementation of FIDO2/WebAuthn authentication covering the registration, login, and account recovery processes using fingerprint biometrics, with the administrative service feature of submitting Surat Keterangan Tidak Mampu (SKTM) as a testing medium. The system is built on a prototype scale using dummy data without integration with external government systems. The method used is Research and Development (R&D) with a three-iteration Prototyping model. The system is developed using a client-server architecture with React.js on the frontend, Node.js and Express.js on the backend, MongoDB as the database, and the SimpleWebAuthn library for the implementation of the WebAuthn protocol. Evaluation of the iterative prototyping model implementation shows an improvement in system feasibility, where the achievement rate of system aspects in the initial evaluation (Iteration 1) was only 50% fulfilled (5 out of 10 aspects) and successfully increased to 100% (all 10 aspects fulfilled) in the final evaluation (Iteration 3). The results of functional testing using Black Box Testing on eleven scenarios show that all features function according to the expected results. Security testing on three threat scenarios, namely phishing, replay attack, and database breach simulation, proves that the system is capable of withstanding all these threats through origin binding mechanisms, one-time challenge, counter incrementing, AES-256-CBC encryption, and the complete elimination of passwords from the system.

Keywords: FIDO2, WebAuthn, Passwordless Authentication, System security, Kelurahan administrative services