

**Passkey (WebAuthn)-ზე დაფუძნებული ფიზინგ-რეზისტენტული
ავთენტიფიკაციის სისტემის დიზაინი და იმპლემენტაცია
განაწილებულ .NET გარემოში**

დომიტრი დონდოლაძე

სამაგისტრო ნაშრომი წარდგენილია ილიას სახელმწიფო უნივერსიტეტის ბიზნესის,
ტექნოლოგიისა და განათლების ფაკულტეტზე პროგრამული ინჟინერიის
მაგისტრის აკადემიური ხარისხის მინიჭების მოთხოვნების შესაბამისად

პროგრამული ინჟინერია

ნაშრომის ხელმძღვანელი: შოთა ცისკარიძე, ილიას სახელმწიფო უნივერსიტეტის
ასოცირებული პროფესორი

პროექტის ხელმძღვანელი: ავთანდილ რუხაძე



ილიას სახელმწიფო უნივერსიტეტი
თბილისი, 2026

განაცხადი

როგორც წარდგენილი სამაგისტრო ნაშრომის ავტორი, ვაცხადებ, რომ ნაშრომი ჩემი ორიგინალური ნამუშევარია და არ შეიცავს სხვა ავტორების მიერ აქამდე გამოქვეყნებულ, გამოსაქვეყნებლად მიღებულ ან დასაცავად წარდგენილ მასალებს, რომლებიც არ არის მოხსენიებული ან ციტირებული სათანადო წესების შესაბამისად.

დიმიტრი დონდოლაძე

20 ივნისი 2026

მადლობა

მინდა გულწრფელი მადლობა გადავუხადო ჩემს სამეცნიერო ხელმძღვანელს, შოთა ცისკარიძეს, კვლევის პროცესში გაწეული ფასდაუდებელი ხელმძღვანელობისთვის, აკადემიური მხარდაჭერისა და რჩევებისთვის. ასევე, მადლობას ვუხდით ჩემს პროექტის ხელმძღვანელს, ავთანდილ რუხაძეს, ტექნიკური მენტორობისა და სისტემის იმპლემენტაციის პროცესში მოცემული პრაქტიკული რეკომენდაციებისთვის.

განსაკუთრებული მადლობა ილიას სახელმწიფო უნივერსიტეტს, ბიზნესის, ტექნოლოგიისა და განათლების ფაკულტეტს ამ კვლევისთვის საჭირო რესურსებისა და გარემოს უზრუნველყოფისთვის. დასასრულს, მადლიერი ვარ ჩემი ოჯახის წევრებისა და მეგობრების მათი მუდმივი გამხნევებისა და მხარდაჭერისთვის.

დიმიტრი დონდოლაძე

აბსტრაქტი

პაროლებზე დაფუძნებული ავთენტიფიკაცია დღემდე რჩება მომხმარებელთა იდენტიფიკაციის ყველაზე გავრცელებულ მექანიზმად, მიუხედავად იმისა, რომ იგი დაკავშირებულია ფიშინგის, ანგარიშების გატაცებისა და სხვა ტიპის კიბერუსაფრთხოების რისკებთან. ბოლო წლებში განვითარებულმა Passkey (WebAuthn) ტექნოლოგიამ წარმოადგინა უფრო უსაფრთხო ალტერნატივა, თუმცა მისი პრაქტიკული დანერგვა ორგანიზაციებსა და პროგრამულ სისტემებში ჯერ კიდევ შეზღუდულია.

წინამდებარე ნაშრომის მიზანია Passkey (WebAuthn) ტექნოლოგიის შესწავლა, მისი უპირატესობებისა და შეზღუდვების ანალიზი, და .NET პლატფორმაზე დანერგვის პრაქტიკული ასპექტების კვლევა. ნაშრომში განხილულია WebAuthn და FIDO2 სტანდარტების მუშაობის პრინციპები, მათი ინტეგრაცია OpenID Connect (OIDC) პროტოკოლთან და არსებული ავთენტიფიკაციის მექანიზმებთან შედარება უსაფრთხოების, გამოყენებადობისა და დანერგვის სირთულის თვალსაზრისით.

კვლევის პრაქტიკული ნაწილის ფარგლებში განხორციელებულია Passkey-ზე დაფუძნებული ავთენტიფიკაციის სისტემის რეალიზაცია .NET გარემოში, რომელიც წარმოადგენს აღნიშნული ტექნოლოგიის დანერგვის საჩვენებელ მაგალითს. ჩატარებული ანალიზისა და ექსპერიმენტების საფუძველზე შეფასებულია მიდგომის უსაფრთხოება, წარმადობა და გამოყენებადობა რეალურ პროგრამულ სისტემებში.

მიღებული შედეგები აჩვენებს, რომ Passkey (WebAuthn)-ზე დაფუძნებული ავთენტიფიკაცია წარმოადგენს ფიშინგის მიმართ უფრო მდგრად ალტერნატივას ტრადიციულ ავთენტიფიკაციასთან შედარებით და ეფექტურად შეიძლება იქნეს ინტეგრირებული .NET პლატფორმაზე დაფუძნებულ თანამედროვე პროგრამულ სისტემებში. **ძირითადი საძიებო სიტყვები:** Passkey, WebAuthn, ფიშინგ-რეზისტენტობა, .NET, განაწილებული სისტემები, OIDC, FIDO2, Redis.

Abstract

Password-based authentication remains the most widely used mechanism for identifying users, despite being associated with phishing, account compromise, and other cybersecurity risks. In recent years, Passkey (WebAuthn) technology has emerged as a more secure alternative; however, its practical adoption in organizations and software systems remains limited. The aim of this thesis is to study Passkey (WebAuthn) technology, analyze its advantages and limitations, and investigate the practical aspects of its implementation on the .NET platform. The thesis examines the operating principles of the WebAuthn and FIDO2 standards, their integration with the OpenID Connect (OIDC) protocol, and compares them with existing authentication mechanisms in terms of security, usability, and implementation complexity. As part of the practical component of the research, a Passkey-based authentication system was implemented in a .NET environment, serving as a reference example for the adoption of this technology. Based on the conducted analysis and experiments, the security, performance, and applicability of the proposed approach in real-world software systems were evaluated. The obtained results demonstrate that Passkey (WebAuthn)-based authentication provides a more phishing-resistant alternative to traditional authentication methods and can be effectively integrated into modern software systems built on the .NET platform. **Keywords:** Passkey, WebAuthn, phishing resistance, .NET, distributed systems, OIDC, FIDO2, Redis.