UNIVERSITY OF ECONOMICS – VARNA
FACULTY OF COMPUTER SCIENCE
DEPARTMENT OF INFORMATICS

Petar Dimitrov Dimitrov

Universal two-factor authentication for protecting web-based information systems

AUTHOR'S SUMMARY

of dissertation work
for awarding the educational and scientific degree "Doctor" in the doctoral program "Informatics"
professional field
4.6. "Informatics and Computer Sciences"

Scientific supervisor:
Prof. Dr. Pavel Petrov

Varna
2026

The dissertation is 168 pages long, including 26 figures and 5 tables. The bibliography includes 129 sources.
The main results of the research are presented in scientific publications - 3 scientific articles and 4 scientific reports.
The dissertation was discussed and approved for defense before a scientific jury at a meeting of the Department of Informatics at the Faculty of Informatics of the University of Economics - Varna on January 21, 2026.

Scientific jury:
1. Internal members
Prof. Silvia Parusheva, PhD, UE-Varna, parusheva@ue-varna.bg
Assoc. Prof. Ivan Kuyumdzhiev, PhD, UE-Varna, ivan_ognyanov@ue-varna.bg

2. External members
Prof. Georgi Petrov Dimitrov, PhD, УниБИТ, g.dimitrov@unibit.bg
Assoc. Prof. Boyan Kolev Zhekov, УниБИТ, b.jekov@unibit.bg
Prof. Evdokiya Nikolaeva Sotirova, PhD, Burgas State University "Prof. Dr. Assen Zlatarov", esotirova@btu.bg

The defense of the dissertation will take place on..... at..... hours in hall..... of the University of Economics - Varna at a meeting of the Scientific Jury, appointed by Order No..... of the Rector of the University of Economics - Varna.
The materials for the defense are available to those interested on the website of the University of Economics - Varna, https://www.ue-varna.bg

I. GENERAL CHARACTERISTICS OF THE DISSERTATION

1. Relevance of the study

Over the past decade, digitalization has established itself as a major driver of economic and social development, with web-based information systems being implemented in a significant number of public spheres – e-government, healthcare, banking, education and e-commerce. The growing importance of these systems is accompanied by an increase in cyber threats aimed at compromising user identity and access to sensitive information.

The most vulnerable element in web system security traditionally remains the password, and despite its long-standing use as the primary authentication method, its use has a number of disadvantages:

- can easily be stolen through various types of attacks, including phishing and the use of malware;
- easy and widespread passwords are often used, which are subject to various types of attacks (e.g. brute force and dictionary attacks);
- users often reuse the same password across multiple systems, which increases the risk of mass breaches through credential stuffing attacks.

According to the Verizon Data Breach Investigations Report 2023 compromised credentials are at the root of over 40% of successful breaches – distinguishing between general incidents and specific web attacks. For broader context, the 2024 report found that the "human factor" (errors, phishing, compromised passwords) was a factor in approximately 68% of breaches. Numerous studies have shown that traditional authentication with a username (or email address) and password demonstrates low reliability as a means of protecting sensitive data and accessing services in the modern digital environment. Traditional password-based authentication methods have been identified as a critical security vulnerability, as weak, reused, or compromised passwords are among the main attack vectors. Passwords have proven to be an insufficient defense against cybercrime, leading to the conclusion that many users prioritize usability over security.

In an attempt to overcome this problem, additional security mechanisms called two-factor authentication (2FA) are being implemented – usually through one-time codes (either via SMS or via a mobile app). While increasing security and making access to sensitive information or services more secure, these mechanisms also have disadvantages:

- SMS messages can be intercepted through specific types of attacks on mobile infrastructure;
- consumer devices are vulnerable to SIM swapping attacks, in which the attacker manages to transfer the victim's phone number to a SIM card in their control and thus gains access to one-time authentication codes sent via SMS;
- the introduction of additional codes creates significant inconvenience for users.

In order to solve the above problems, the FIDO Alliance was created, which, through the FIDO2, WebAuthn and CTAP2 standards, formulated an approach for introducing passwordless authentication, aimed at increasing security and reducing dependence on traditional passwords. An approach was proposed in which users authenticate with cryptographic keys protected in hardware or software authenticators, without the need to remember and enter passwords. This significantly increases security by eliminating the risk of phishing and password theft, and at the same time improves the user experience.

The term “universal two-factor authentication” (U2F) is used in accordance with the original concept of the FIDO Alliance from the period 2014-2018 and in this thesis serves as a basis for the subsequent research and integration of the extended standard FIDO2/WebAuthn. In the context of the thesis, the term “universal two-factor authentication” refers to the unified authentication model based on cryptography through public and private keys and standardized protocols, rather than to a specific implementation limited within a single system.

2. Research thesis

The research thesis of the dissertation is that the FIDO2/WebAuthn standards allow for the construction of a universal and practically applicable model for strong authentication in web-based information systems, which simultaneously increases security and maintains a high degree of usability. Through cryptographic authentication with public and private keys and other methods specific to the standard, WebAuthn eliminates major classes of attacks (phishing, credential stuffing and MitM), typical of password-based solutions, and allows implementation in real institutional environments without fundamentally changing their architecture.

3. Goals and objectives of the study

The goal on the present dissertation is to is develop a conceptual and architectural model for universal two-factor authentication in web-based informational systems, founded on the FIDO2 and WebAuthn standards, which provides high level of cryptographic protection, resilience against contemporary attacks and practical applicability in real life institutional environments. Within the study, special attention is given on usability and accessibility for the end users, so that the proposed model is not only safe, but also usable in everyday practice.

To achieve the goal set in the dissertation, the following main objectives are set:

- conducting a systematic analysis of existing user authentication approaches and their limitations; researching the architectural principles and standards related to FIDO2/WebAuthn and their integration with existing identity management systems;
- design and modeling of an architecture for a two-factor authentication system with clearly defined logical, communication and data-oriented components;
- analysis of risks, threats and future trends in the security of passwordless systems, including in the context of post-quantum cryptography, considered in an analytical and prognostic aspect.

4. Object and subject of research

The object of the research is the protection of web-based information systems that process sensitive data and require reliable user authentication.

In the framework of this work, a "web-based information system" is understood as a multi-layered application, accessible via a web browser or web client, that uses HTTP(S) as a transport protocol, centralized server logic, and a database for storing and processing information. It is characteristic of this type of system that access to their functionalities is achieved through standard web technologies (HTML, CSS, JavaScript) and they often serve a large number of remote and heterogeneous users.

The consideration of web-based information systems in the study is conditioned by several factors. First, this type of systems is widespread in the context of e-government, education and cloud services, providing remote access to critical data and functions for a large number of users. Second, web applications traditionally rely on password-based authentication, which makes them significantly vulnerable to multiple types of attacks. Third, standards such as FIDO2/WebAuthn are designed for the web environment and provide a built-in mechanism for replacing passwords with cryptographic keys. In this context, web-based systems represent the most suitable and relevant environment for analyzing and implementing a universal model for strong authentication.

The subject of the research covers architectural solutions, cryptographic protocols and technologies for implementing universal two-factor authentication based on FIDO2 and WebAuthn, as well as the integration of modern methods for protecting web applications from current attack vectors, such as phishing, replay attacks, session compromise and credential abuse.

The aim of this dissertation is to develop a conceptual model and architecture for universal two-factor authentication of users in web-based information systems, based on the FIDO2/WebAuthn standards, which provides a high level of cryptographic protection by using modern algorithms and protocols, consistent with the best practices in information security. The model is conceptually aimed at

achieving resilience to the most common cyberattacks, including phishing, replay attacks and credential stuffing, by implementing mechanisms for secure verification and session management. In the context of standardization and compatibility with different platforms, the paper proposes an integration approach based on the FIDO2 and WebAuthn standards, which ensures the applicability of the developed architecture to a wide range of web systems and guarantees compatibility with current browsers and devices. Special attention is given to usability and accessibility for end users, by developing interface solutions and procedures that minimize barriers to implementing two-factor authentication and increase user satisfaction and safety.

5. Research Methodology

The methodological apparatus of the study includes the following research methods and techniques:

- Comparative analysis – to evaluate traditional 2FA methods versus WebAuthn in terms of security, convenience, and implementation.
- Systemic approach – for modeling the architecture and interaction between components.
- Modeling and prototyping – to build a test environment and demonstrate various scenarios (registration, authentication).
- Logical analysis and scenarios – to describe data flows, attacks and protection mechanisms.

The methodology includes both theoretical analysis and practical implementation by building a prototype of a two-factor authentication system with an integrated WebAuthn server and a real database.

This research is implemented within certain limitations that should be taken into account when interpreting the results and conclusions drawn. First, the dissertation focuses on web-based information systems and the FIDO2/WebAuthn standards in the context of a web environment, which means that the analysis and

the proposed architecture do not fully cover the specific features of other types of systems.

Secondly, the practical implementation and experimental part of the study are limited to a specific technological platform (PHP/MySQL and standard web browsers), which allows for a detailed analysis of WebAuthn integration, but does not claim to be exhaustive in terms of all possible programming languages and environments. The conclusions drawn regarding the applicability and effectiveness of the model should be considered valid within the chosen technological configuration.

The study does not aim at a comprehensive formal verification of the cryptographic protocols used, but is based on established standards and existing formal analyses published by the W3C, FIDO Alliance and the academic community. For this reason, the work focuses on the architectural, integration and application aspects of FIDO2/WebAuthn, and not on the development of new cryptographic primitives. In terms of usability and user experience, the analysis is based mainly on existing empirical research and limited observations within the framework of the prototype implementation, without conducting large-scale user experiments with a representative sample. In this sense, the conclusions made about UX should be considered indicative and as a basis for future more in-depth research. The consideration of future trends, including post-quantum cryptography, is primarily prognostic and analytical in nature and does not include experimental evaluation of real post-quantum implementations within WebAuthn, since such standardized solutions are still under development and evaluation at the time of the study.

5. Approbation

The testing of the obtained results was carried out by developing and implementing a working prototype for WebAuthn authentication in the university system WSDB of the University of Varna, as well as by publishing and presenting results in 3 scientific articles and 4 scientific reports. The practical implementation

includes scenarios for authenticator registration, two-factor authentication and use of the cryptographic key for signing academic data.

II. STRUCTURE OF THE DISSERTATION THESIS

The dissertation consists of an introduction, three chapters and a conclusion and is 168 pages long, including 26 figures and 5 tables. The bibliography includes 129 literary sources.

Contents:

Chapter III. Implementation of WebAuthn in the web-based information system of the University of Economics – Varna

3.1 General characteristics of the University of Economics – Varna

3.2. Integrating WebAuthn into the existing PHP/MySQL environment

3.3. System components

3.4. Server configuration and system implementation

3.5. User registration and authentication

3.6. Hardware devices

3.7. Possibilities for implementing WebAuthn in the educational process of higher education institutions

Conclusion

References

Reference for contributions in the dissertation work

List of publications on the dissertation

III. SUMMARY OF THE DISSERTATION

Chapter I. Theoretical and practical prerequisites for the implementation of WebAuthn

The use of more and more information systems, platforms and applications in both personal and professional life expands the possibilities for remote work, electronic services and data processing, but at the same time increases the exposure to cyber risks. In the dissertation, this reality is considered as a starting point for the study of authentication as a critical access control mechanism which the protection of sensitive information and the reliability of web-based information systems depend on. Organizations are faced with the need to simultaneously maintain high usability and at the same time implement security mechanisms that are resistant to current attacks against sensitive and authentication data.

One of the earliest and most widespread methods of restricting access is the password. The dissertation traces its historical adoption as a means of authentication, including its introduction into multi-user computer systems and the formation of the centralized authentication model. It is argued that although the password is technologically simple and easy to implement, it makes security dependent on human factors and the quality of organizational practices for its creation, storage, and use.

Over time, passwords begin to show their limitations. The dissertation emphasizes that in real-world conditions, many users use short or predictable passwords and often reuse them in other systems. This creates the prerequisites for a number of attacks, as well as for large-scale compromises of accounts when data leaks from one service and subsequent "transfer" of the risk to other services. It is this complex of vulnerabilities that motivates the transition to mechanisms that reduce or eliminate the dependence on "shared secrets" and limit the possibility of phishing and reuse of compromised credentials.

The first subsection, "**Methods for storing authentication data**" establishes that authentication security does not depend solely on the chosen login mechanism, but also on the way the system stores and processes authentication data. The main approaches to storing user IDs and passwords are presented and the risks associated with them are analyzed. It is emphasized that the historical transition from storage in clear-text to hashing and salting is key to reducing the consequences of breaches, but does not solve the fundamental weaknesses of the password model itself.

The early approach of storing passwords in plain text, typical of the first multi-user systems, is described. It is shown that centralized storage of passwords in a readable format leads to critical vulnerabilities. such as the fact that a minimal configuration error or incorrect access control can result in a mass compromise of user accounts. On this basis, an important principle is formulated, which is also developed in the following chapters of the dissertation, namely, the storage function and the verification function of authentication data should be implemented in such a way that even in the event of partial compromise, secret strings that could lead to

unauthorized access are not revealed. It is noted that although this approach is considered incompatible with modern practices, there are still systems today in which, due to technical and organizational shortcomings, the storage of passwords without adequate cryptographic protection is allowed, which in the context of the dissertation is considered a high-risk factor.

The introduction of cryptographic approaches to password protection is analyzed and the role of hash functions and salting in reducing the risk of offline cracking in the event of database leaks is argued. Historical examples are also presented, which show that algorithms considered reliable in one period may be inadvisable for use with the increase in computing power and the emergence of specialized hardware. This analysis prepares the logical transition to the thesis of the dissertation work that even with correct hashing and salting, the password model remains structurally vulnerable to various types of attacks, which necessitates the search for approaches that replace passwords with cryptographic certificates.

In the subsection "**Qualified electronic signature as a means of authentication**" of the dissertation, the qualified electronic signature (QES) is examined as a technological instrument with the highest legal value within the European Union and in particular in the Bulgarian legal framework. The analysis emphasizes that QES is based on a classical public key infrastructure (PKI) and asymmetric cryptography and provides not only authentication, but also irrevocability in legally significant actions. At the same time, it is argued that the use of QES as a mass mechanism for everyday authentication in web applications also has disadvantages, such as dependence on specialized devices/carriers, issuance and maintenance procedures, as well as specific user and organizational requirements. This comparative analysis serves as an intermediate step in the dissertation to justify the need for solutions that combine high cryptographic security with better usability and operational applicability in broad user environments.

In the subsection "**Critical analysis of vulnerabilities and evolution of authentication technologies**" of the dissertation, the evolution of security is examined as a constant dynamic between protective measures and techniques for

their circumvention. It is emphasized that protection must be systematic and cover the entire spectrum of attack vectors. On this basis, examples of large-scale breaches and leaks of passwords and hashes are presented, which demonstrate the consequences of dependence on static authentication data. A key conclusion is drawn, which is leading for the dissertation, namely that the reuse of passwords, storage deficiencies and attacks based on social engineering lead to a "chain" risk, in which compromising one service can lead to compromising multiple others.

Current attack vectors against authentication mechanisms are systematized, emphasizing that attackers combine technical and social approaches. Brute force attacks, dictionary attacks, repeat attacks, phishing campaigns, as well as scenarios for compromising sessions and intermediate components are considered. The analysis shows that increased computing power and the availability of databases of already expired passwords significantly lower the practical barrier to attack, which again points to the need for mechanisms that, by design, reduce the benefit of stolen credentials and limit the possibility of replacing the authentication context.

In the subsection "**Aspects of FIDO2 implementation and user acceptance**" of the dissertation, it is discussed that passwordless and phishing-resistant approaches based on FIDO2/WebAuthn offer a significantly higher level of security compared to traditional methods, but their implementation in a real environment is determined by architectural, organizational and human factors. Issues such as the choice of authenticators (platform and external), user experience, device registration policies, management of multiple devices, as well as restoration of access in case of loss or replacement of an authenticator are analyzed. Attention is paid to the trend towards large-scale support of passkeys in modern platforms and browsers, which creates favorable conditions for mass use. These aspects are used as the basis for the subsequent chapters of the dissertation, in which a model for the integration of WebAuthn is developed and its practical implementation in a real university web-based information system is demonstrated.

Chapter II. Authentication model based on FIDO2 and WebAuthn standards

In the second chapter of the dissertation, a model for strong two-factor authentication for web-based information systems, based on FIDO2 and WebAuthn, is developed, with the focus on the balance between three mutually dependent requirements, namely security, scalability and user convenience. It is shown that in real institutional environments the authentication architecture must simultaneously counteract phishing, replay attacks, avoid compromising sensitive data and serve high concurrent activity without performance degradation, and be usable enough to be widely accepted by users. On this basis, goals for the implementation of a two-factor authentication system are formulated, namely:

- ensuring that only authorized users have access through secure communication and cryptographic authentication using asymmetric methods;
- ensuring scalability through efficient storage and fast verification of public keys and optimized database operations;
- increasing convenience by reducing reliance on complex passwords and by using authentication tools integrated into the user ecosystem, including biometric data and local verification mechanisms.

The first subsection, "**FIDO2/WebAuthn – role in the strong authentication model**", justifies the choice of FIDO2/WebAuthn as a logical response to the systemic weaknesses of password-based authentication and traditional 2FA approaches. It is shown that with passwords the risk is concentrated in a static string, the quality of which depends on user habits and which can be stolen, reused or compromised in case of a breach in storage. It is shown that FIDO2 combines WebAuthn (browser API) and CTAP2 (client-authenticator communication protocol), replacing the password and/or one-time codes with asymmetric cryptography and a "challenge-signature" model. When an authenticator registers, a key pair is generated for the specific service (Relying Party), with the private key remaining in a secure environment on the device/authenticator and not

leaving this environment, and only the public key being stored on the server. During authentication, the server sends a unique cryptographic challenge, which is signed locally and validated using the public key. It has been argued that this architecture changes the threat model – compromising the database does not lead to possible offline password cracking, reusing credentials becomes practically infeasible, and phishing is limited by design by binding authentication to the origin and service identifier. In comparison, it has been pointed out that solutions such as SMS-OTP and TOTP, although adding a second factor to authentication, remain vulnerable to attacks on the telecommunications channel and to phishing through redirection and social engineering, respectively, as they rely on the user transmitting and/or entering codes.

The second subsection, "**Conceptual Model**" formalizes the participants, functional boundaries, and logical relationships in the universal two-factor authentication system, emphasizing that the goal of the conceptual level is not to describe specific formats and protocol fields, but to clearly distinguish roles and responsibilities. The main logical units are defined, namely user, client application (browser/mobile application), authenticator, server (Relying Party) and a public key repository. The user initiates registration and authentication by confirming operations through an action that guarantees conscious participation (for example, pressing a button, biometrics, or entering a PIN). The client application mediates between the web application and the authenticator, managing the WebAuthn interface and transferring the data to the server. The authenticator stores the private key in a secure environment and performs cryptographic operations, refusing to sign without explicit user participation, and if necessary, providing the so-called attestation, which allows the server to establish characteristics and trust in the devices/authenticators used. The server generates unique cryptographic challenges, stores public keys, and validates signatures, and the database contains public keys and metadata, so that even if it is compromised, sensitive data is not compromised. The relationship with assurance levels is addressed through a framework that defines levels of authentication confidence, with the highest level requiring phishing -

resistant authenticators and a non-transferable private key – a requirement that is achieved precisely through FIDO2/WebAuthn. The conceptual model also specifies the cryptographic primitives used and the roles of the algorithms – digital signatures (e.g. ECDSA or RSA), hashing (e.g. SHA-256), and random value generation for cryptographic challenges.

In the third subsection "**Logical Model"** we move from the abstract description to the formalization of the data and the dependencies between them, using the ER representation as the basis for a relational structure independent of a specific DBMS. A minimalistic but functionally sufficient division of the data into two main tables is shown:

- user table (identifier, unique username and contact information)
- a table of FIDO credential records associated with a specific user.

Authenticator details are described, namely:

- device identifier /credentials
- connection to the user
- key identifier (keyHandle/credential identifier)
- public key
- certificate/certification data (when used)
- counter (signCount/counter) to detect repetition or cloning.

It is emphasized that the structure supports multi-device scenarios, as a user can have more than one registered authenticator, which is critical for the resilience of the authentication mechanism in the event of the loss of one of the authenticators. Additionally, opportunities for higher manageability and security are outlined, including logging of successful/failed authentication attempts with timestamp and IP address, credentials and prioritization of backup devices, history of keys and certificates, binding to IP/geolocation for risk analysis, as well as mechanisms for logical deletion (soft-delete) that limit dangerous operations and support database auditing.

The fourth subsection, "**Communication Model**" describes the semantics and order of message exchange between participants, examining when and how the

server creates a challenge, how the client passes it to the authenticator, how the authenticator returns a signed response (assertion), and how the server validates the signature using the public key from the repository. It is shown that the model combines the protocol requirements of WebAuthn/CTAP2 (data presentation formats, attestation, user verification) with infrastructure requirements such as working over HTTPS/TLS, correct generation of cryptographic challenges, and session management. The registration flow is described as a sequence in which the authenticator locally generates a key pair, the public key is transmitted over a secure channel, the server validates and stores it, returns confirmation of successful registration, and for multiple devices the public key is associated with the user as a separate record. The data flow during authentication is described by selecting a registered device/authenticator, signing a challenge with the private key and verification by the server against the corresponding public key, while maintaining mechanisms for logging device, time and IP for subsequent analysis. Attention is paid to the fact that protecting communication via TLS/HTTPS is a mandatory condition, since the protocol ensures confidentiality, integrity, prevents eavesdropping and data substitution in the channel and is a prerequisite for WebAuthn to be executed in a protected context. It is emphasized that incorrect TLS configuration (outdated versions, weak ciphers, invalid certificates) can compromise the entire security of the solution, regardless of the reliability of the authenticator.

The fifth subsection, "**Structure and mechanisms of the WebAuthn and CTAP2 protocols**" examines the internal structure of the protocol data and the interaction between the web layer and the authentication device. It is shown that WebAuthn defines the standardized interface for web applications and browsers, while the actual communication to the authenticator is carried out through CTAP2, with the browser acting as an intermediary between the application and the hardware/platform. It is indicated that CTAP2 uses a compact binary serialization format (CBOR) and supports multiple transport mechanisms (USB, NFC, and Bluetooth Low Energy), which is key to the universal applicability of the approach across different client environments. Also described are basic CTAP2 operations

that manage registration and authentication, including creating credentials (makeCredential), obtaining a login proof (getAssertion), securing with a local PIN, and retrieving device capabilities. From the WebAuthn side, the key data structures that provide context binding and verifiability are discussed:

- user data, which includes challenge, origin, and type of operation;
- authenticator data, which contains a hash of the service identifier (rpIdHash), status flags such as user verification, signature counter (signCount), and registration credentials;
- and an attestation object that allows the server to validate device characteristics and trust when policies require it.

It is emphasized that it is the combination of "origin binding " and the RP-ID makes the signature unusable outside the real system, and attestation is especially relevant for environments with high requirements for control over the types of permissible authenticators.

The sixth subsection, "**Security and Performance Analysis**" systematically evaluates the countermeasures built into the protocol, as well as the effects on latency, throughput, and server infrastructure load. From a security perspective, it is concluded that WebAuthn eliminates shared secrets and limits the consequences of storage breaches, since public keys and metadata are stored on the server, rather than passwords or equivalent secrets. It is shown how phishing is addressed by cryptographically binding to the domain and service identifier, replay attacks are limited by one-time challenges and counters, and MitM attacks are reduced by a combination of a secure transport layer (HTTPS/TLS) and signing of operation context parameters. Scenarios such as device theft/cloning are considered, and it is stated that the protocol requires a non-transferable private key and allows local user verification (biometrics or PIN entry) that is not carried over to the application layer. The organizational side of security is also emphasized, namely that resilience in a real-world environment depends on policies for acceptable authenticators, device lifecycle management, monitoring and incident response. In addition, future challenges are discussed, such as possible advanced attacks in which compromising

the client-authenticator interaction can lead to session theft, as well as the risks that quantum computing poses to algorithms such as RSA and ECDSA, which necessitates planning for a transition to post-quantum or hybrid string signing schemes.

In terms of performance, it is shown that the evaluation is closely related to the prototype developed in the dissertation, and that the measurement results are used to calibrate parameters such as algorithm selection, TLS/HTTPS configuration and database optimizations. The WebAuthn process sequence (challenge generation and sending, browser-authenticator interaction via CTAP2, server signature verification) is examined and it is specified that different transport mechanisms have different contributions to latency (USB with the lowest latency, NFC and BLE with additional delays due to initialization and connection latency). It is emphasized that the choice of cryptographic algorithm has a direct impact on the load in mass simultaneous authentications, with more efficient configurations allowing better scalability in environments with multiple active users. Within the framework of optimization and scalability, engineering approaches to accelerate storage and cryptographic operations are described, such as indexing by user and authenticator ID, logical table partitioning, caching of static elements such as public keys and metadata, parallelization and asynchronisation in signature verification and message validation, pre-checking the structure before cryptographic processing, as well as infrastructure solutions such as clustering and load balancing, database replication, and the use of caching for static client components.

The seventh subsection, "**Choosing a suitable authenticator**" analyzes the impact of the authenticator type on speed, convenience, and security. A distinction is made between hardware authenticators (USB, NFC, Bluetooth) and platform/biometric solutions, emphasizing that the choice should be based on the required level of assurance, the context of use, and the user profile. It is noted that USB authenticators provide the lowest response times and a high degree of control, NFC solutions add latency due to the contactless channel, and BLE scenarios include additional latency for session establishment. Biometric sensors provide fast and

intuitive authentication, with the essential point being that the comparison of biometric templates is performed locally and the key remains in a secure environment. It is argued that in institutional environments, a hybrid model is often appropriate, in which critical profiles and administrative access use hardware authenticators, and mass users use platform/biometric authenticators, with backup means provided for restoring access.

The eighth subsection "**Integration and operational issues when implementing FIDO/WebAuthn in large institutional environments**" shows that successful implementation requires not only technological integration, but also an organizational framework for management, support and acceptance by users. It is emphasized that the institutional environment is characterized by heterogeneous devices, different technical literacy and the need for compatibility between web and mobile platforms, which requires manageable policies and sustainable processes. The approach for integration with existing identity and access management systems, including centralized authentication schemes, user directories and federated models, is considered, arguing that the optimal effect is achieved when adding WebAuthn at the identity provider level, and not as an isolated functionality in a separate application, as this provides a single point of authentication, unified key management and compatibility between multiple services.

The integration should provide for secure and high-performance storage of authenticator public keys and metadata, indexing by user and identifier of credential data, as well as mechanisms for caching and logical structuring of data at large scale. Attention is paid to the authenticator lifecycle as a key operational challenge, as clear procedures for registration, revocation, temporary blocking and restoration of access are needed, and mandatory registration of a backup authenticator and the possibility of remote deactivation through identity management systems are recommended. For scenarios with remote users, flexible methods for re-authentication of identity are outlined that combine security and operational efficiency.

It is also shown that user adoption depends on the quality of the user experience. Intuitive registration, clear instructions at each step and seamless use

across platforms are required, and measurable metrics can be used (registration time, authentication time, percentage of successful logins without technical assistance). The importance of constant monitoring and auditing of authentication events is emphasized, including logging of successful and unsuccessful attempts, devices used, location and level of trust of the session, as well as the possibility of integration with systems for analysis and early detection of anomalies. Operational indicators for implementation management are also defined (percentage of successfully registered devices, average time to restore access, incidents with lost/compromised authenticators, frequency of use of backup methods), and it is argued that their regular reporting helps optimize processes. In conclusion, it is concluded that implementation in large institutions requires a balanced approach between technological reliability, operational efficiency and user accessibility, and success depends on both the right choice of protocols and devices, and on the organization's ability to manage the authenticator lifecycle, conduct training and maintain a high level of adoption. As a logical continuation, it is indicated that the next chapter presents the practical implementation of FIDO/WebAuthn in a university information system, including integration with the current infrastructure, the processes of registration and management of authenticators and the achieved results of its implementation.

Chapter III. Implementation of WebAuthn in the web-based information system of the University of Economics – Varna

The third chapter of the dissertation presents the practical implementation of WebAuthn in a real web-based institutional environment – the information system of the University of Economics – Varna. The chapter is of an applied nature and shows how the strong authentication model developed in the second chapter can be integrated into an existing infrastructure with minimal risk, without service interruption and while maintaining compatibility with legacy components. The organizational context and evolution of university systems, the chosen architectural strategy for integration into a PHP/MySQL environment, the key technical

components and server configurations, as well as user flows for registration and authentication are examined. The final part demonstrates the possibility of the technology to upgrade authentication and be used as a mechanism for cryptographic authentication of critical actions in the educational process, with an emphasis on the protection of data generated in the academic environment.

The first subsection "**General characteristics of the University of Economics – Varna**" describes the institutional environment in which the implementation is implemented, and argues why a university information system is suitable for validating WebAuthn in the context of diverse users and high requirements for availability and security. University of Economics – Varna is a higher education institution with established practice in the use of digital technologies for managing educational and administrative processes, with the user profile including thousands of students, international students and a significant academic and administrative staff. This heterogeneity places demands not only on access protection, but also on the convenience and reliability of authentication mechanisms, as the system must work across a wide range of devices, browsers and user habits. The subsection traces the evolution of information systems at the university through several technological stages, emphasizing how strategic priorities for digitalization and the development of the Internet infrastructure gradually transform the access model – from locally limited solutions to Internet-accessible platforms. The early stage is presented, in which the server infrastructure is based on a single machine with a Novell operating system, which performs identification functions through a username and password and provides file sharing with program code and databases in dBase format, with access limited to computers in the university's local network. The intermediate organizational approach for informing students through terminals in the university building, where they enter a faculty number (at that time still called "album number") and a personal identification number for retrieving grades and personal data, is also described, with each terminal having a separate computer with a network connection to the server. The next stage is related to a project for converting and modernizing the database, through which

the foundations of a more accessible platform are laid, allowing students to access information via the Internet. In this context, the subdomain info.ue-varna.bg is created and a server environment with Linux, a web server with PHP support and a local MySQL database, also used for the ETL process, is built. This evolution is an important prerequisite for implementing WebAuthn because it shows an available web architecture, real users and workload, as well as a clearly expressed need to increase security in a service available on the Internet.

The second subsection, "**Integrating WebAuthn into the existing PHP/MySQL environment**", examines the strategic approach to upgrading the security of the WSDB system without destroying the existing logic and without the need for a complete rewrite of the user module. The source environment is described as a stable PHP/MySQL infrastructure within a WHM/cPanel server, organizationally supported by a specialized structure at the university, with the system virtualized on a local (self-hosted) infrastructure. The dissertation concludes that this infrastructure provides a higher degree of control over data and configuration, but requires disciplined maintenance, strict updates and active protection mechanisms due to constant exposure to external attacks. The main goal of WebAuthn integration is to introduce it as an additional security layer, working in parallel with classic password authentication, so that the implementation is compatible and allows for gradual migration, including scenarios where WebAuthn gradually replaces the password completely or supplements it as a second factor. It is shown that from an architectural point of view this is implemented through an intermediate layer (middleware) that mediates between the web application, the database and the client's browser and performs key functions such as generating cryptographic challenges, verifying signatures and public keys, processing attestation data, as well as managing sessions and responses to the client. In the context of the PHP programming language, the use of specialized software libraries that implement the necessary registration and authentication operations and allow correct processing of protocol structures and their serialization is considered. It is emphasized that this model guarantees a fundamental property of WebAuthn,

namely that the server works only with public keys and signed responses and by design does not have access to the private keys, which remain protected in the user's authenticator. At the server level, the need for all communication to be carried out via HTTPS with TLS, as well as the limitation of operations to a domain allowed in the WebAuthn configuration, is considered as a key condition. This, combined with the signature's binding to the origin, significantly reduces the risk of phishing and replay attacks, as the generated signatures are valid only within the specific domain and context of the operation.

The third subsection "**System components**" describes the architecture of the implemented solution as a set of four main components, which in combination implement universal two-factor authentication:

- client web interface,
- FIDO device (authenticator),
- server logic for authentication
- and a database to store the necessary information.

The client component is implemented with HTML5, CSS and JavaScript, with the main point of integration being the WebAuthn API in the browser. It is shown that the browser acts as a trusted intermediary between the application and the authenticator, initiating registration by calling `navigator.credentials.create()` and initiating authentication by calling `navigator.credentials.get()`. The dissertation emphasizes that, in addition to the purely technical API call, the client layer is also critical for the quality of the user experience. The client layer manages visual messages, instructions to the user, and the handling of errors and retries, for example when the device is not found, when the user interrupts the process, or when authentication fails. The practical aspect of compatibility is also discussed - the need for the solution to work in different browsers and mobile operating systems, which is key for an institutional service with a wide user profile. It is indicated that the system is configured so that in the initial stage it does not require specific authenticator attestation models, which reduces the barriers to implementation and facilitates initial implementation and operation. Attention is also paid to parameters

that affect real usability, such as the setting of response time windows, since excessively short values can lead to unsuccessful processes in certain transport modes, for example, with Bluetooth authenticators. The architectural part also includes an architectural model for implementing WebAuthn in WSDB (Figure 1), which visualizes the interactions between the browser, WebAuthn API, authenticator, server and database and fixes the place of the middleware layer in the overall scheme.

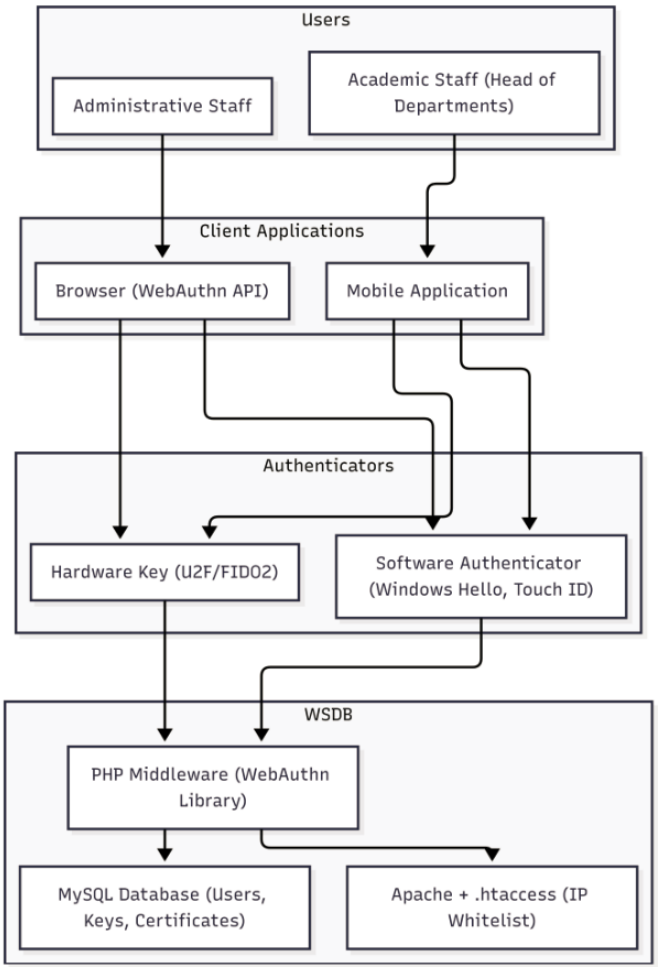

Figure 1WSDB authentication system architecture

Developed by the author

The fourth subsection, "**Server configuration and system implementation**" argues the choice of a web server and the specific configuration as part of the requirements for compatibility and minimal risk during integration. The dissertation assumes that Apache HTTP Server is the most appropriate solution in the specific context, as it is already implemented and maintained within the WHM/cPanel

environment in which the university system operates. It is presented that Apache offers long-term stability, broad ecosystem support and native compatibility with traditional PHP applications, including those that rely on .htaccess and module directives. A comparison with alternatives is made, specifying that although some of them have advantages when serving static content, in the context of a dynamic PHP/MySQL application and when minimal architectural changes are required, Apache in combination with PHP-FPM represents a practical and low-risk solution. It is emphasized that a critical condition for WebAuthn is the availability of HTTPS, which is provided by a TLS/SSL module and appropriate certificate support, and this can be managed effectively in a cPanel environment. The possibility of preserving and upgrading current access restriction policies (e.g., already existing IP restrictions) through configuration mechanisms has also been considered, so that WebAuthn does not replace existing control, but complements it with a modern authentication protocol.

The fifth subsection, "**User registration and authentication**" describes the user flows and engineering solutions for their implementation in WSDB, considering two approaches for registering a FIDO authenticator to a user profile. The first, more common approach, divides registration into two logical steps – first, a base record for the user is created in the database to generate a unique identifier (user ID), and then, upon successful signing by the authenticator, the data for the newly created public key and the identifier of the authentication data are added to this record. It is argued that this facilitates the correct binding of the challenge to a specific user and maintains clear transactional logic during storage. The second approach implements a one-step registration, in which the entered username and password are intercepted and validated before the request for generating a challenge, after which an additional server check for uniqueness of the username is performed and registration continues. The dissertation states that this approach can reduce the number of steps for the user, but requires stricter validation and careful data management. On the client side, the registration process is described as a sequence in which, after entering a user ID, the client requests the registration parameters from the RP server, including a

cryptographic challenge, service identifier, user data, permissible cryptographic parameters, and policies. The browser then initiates the creation of credentials via the WebAuthn API, and the resulting structures are serialized into a suitable transport format and sent to the server for validation and recording. On the server side, the process is described as a two-step process – generating and temporarily storing a challenge for correlation between the request and the response (e.g., in a session variable), followed by accepting the response from the authenticator, verifying the signature and (if available) the attestation data, and finally recording the public key, the credential identifier, and a counter (signCount), which helps protect against replay and detect potential cloning.

The sixth subsection, "**Hardware devices**" examines hardware authenticators as physical carriers of cryptographic keys and as a practical option for users with increased access levels in university and institutional environments. It is shown that their main advantage is the isolated environment for generating and storing the private key, which minimizes the risk of malware and compromise through the operating system and network layers. The dissertation explains that modern FIDO2 authenticators work through the CTAP2 protocol, which defines the communication between the browser/application and the physical device, and the devices can use different interfaces – USB for desktop computers and administrative stations, NFC and Bluetooth for scenarios with mobile devices and users who work with laptops and smartphones. It is described that hardware authenticators rely on secure elements such as Secure Element or TPM to store the private key and perform cryptographic operations internally on the device, so that the private key is not exposed and does not leave the protected environment; only a signature on a unique challenge generated by the system is sent to the server. It is emphasized that this model is particularly suitable for profiles where compromising access would have significant consequences, for example, administrators, employees and teachers with advanced rights.

The seventh subsection "**Possibilities for implementing WebAuthn in the educational process of higher education institutions**" expands the scope of

application of the technology beyond authentication in the system and demonstrates how WebAuthn can be used as a cryptographic mechanism for authenticating and signing critical actions in the educational process, with an emphasis on the assessment of students by teachers. The dissertation first describes the basic, "analog" scenario, in which the process begins with the students taking an exam, the teacher forms a grade on a six-point system and enters it into a pre-prepared list of students, called the "exam protocol". After completing the exam, the teacher also reflects the grades in the so-called "general ledger", which is a structured set of student data organized according to a certain principle, for example, by faculty or form of study. It is indicated that the requisites and requirements for the general ledgers are normatively defined, and the process logically ends at the stage when the student reaches graduation, when an employee checks the availability of all grades according to the curriculum and prepares the diploma, practically transferring the information from the general ledger to the diploma document. On this basis, a model for digitization is proposed, in which WebAuthn is not only used for authentication, but is also used for cryptographic signing of the actions of entering and confirming grades and other academic records. It is described that when entering or confirming a grade, the system generates a unique challenge, which includes identifiers of the discipline, protocol, specific student and time stamp, after which the authenticator signs the challenge, and the server validates the signature against the public key associated with the teacher's profile. Thus, each grade is accompanied by verifiable cryptographic evidence of authorship and integrity of the record, which increases the possibility of performing audits and reduces the risk of unauthorized changes and controversial situations during subsequent checks. The dissertation paper states that the model is applicable not only to assessments, but also to signing examination protocols and ledgers, as well as to other academic documents and actions where organizational rules require increased reliability and traceability. The conceptual model for digitally signing academic records with WebAuthn is illustrated in Figure 2, which visualizes the challenge-signature-verification flow and its relationship to academic data registers.

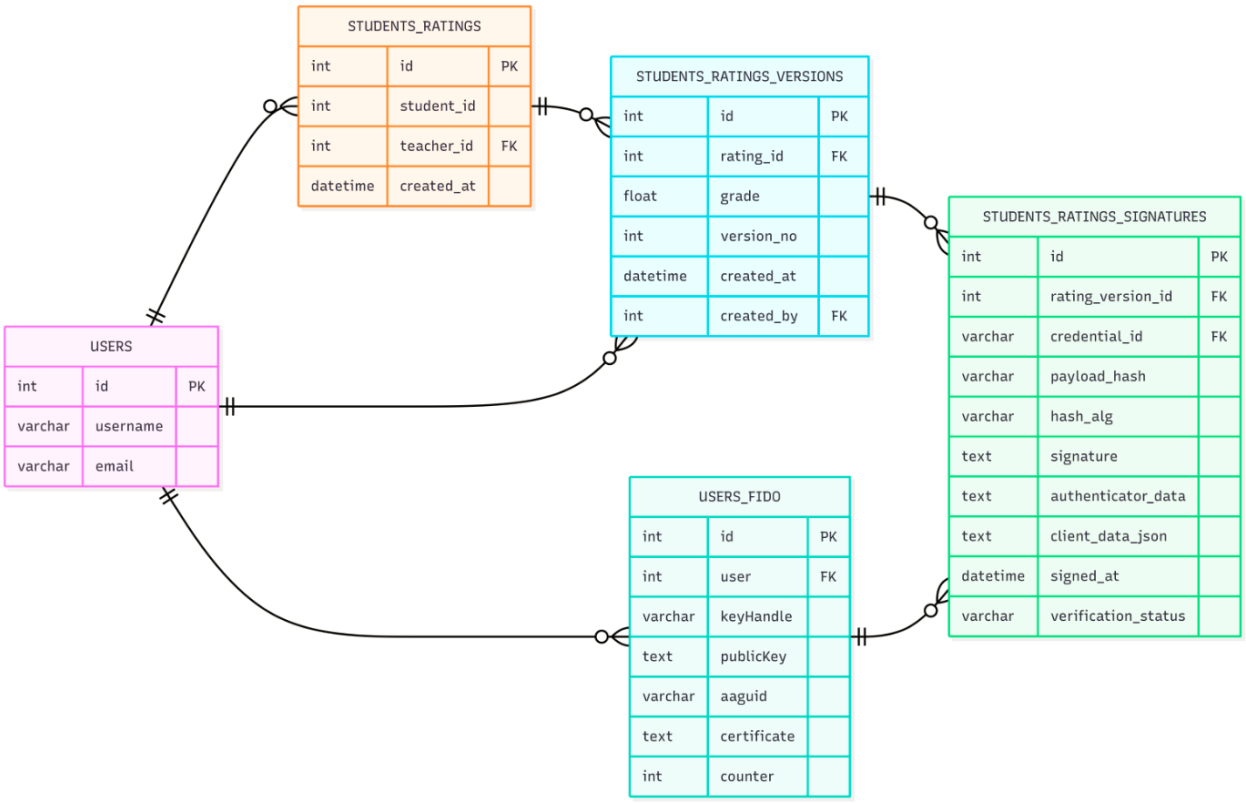

Figure 2Extended relational model for the purpose of signing assessments

In conclusion of the chapter in the dissertation, it is summarized that the implemented implementation demonstrates the practical applicability of WebAuthn as a universal mechanism for strong authentication in web-based systems under real organizational constraints. It is shown that the chosen approach allows upgrading an existing PHP/MySQL environment with minimal invasiveness and maintaining backward compatibility, while simultaneously creating a basis for expansion to scenarios with a higher degree of provability and auditability of critical actions, including in the learning process.

IV. CONTRIBUTIONS

Based on the research conducted in the dissertation, the following scientific and practical contributions can be formulated:

1) The concept of WebAuthn as a new authentication paradigm, overcoming the main vulnerabilities of password-based authentication mechanisms, is theoretically justified.

2) An architectural model for implementing WebAuthn in a university web-based information system has been developed, adapted to the Bulgarian academic context and to the existing PHP/MySQL infrastructure.

3) A practical integration of WebAuthn into a real university information system (WSDB of the University of Varna) has been implemented, through which a complete and working cycle of registration and authentication with FIDO2 compatible authenticators has been demonstrated.

4) A mechanism for cryptographic signing of actions (in particular, entering and signing student grades) based on WebAuthn has been proposed and experimentally validated, which ensures binding of the authenticated identity to a specific action within the university information system.

V. PUBLICATIONS ON THE DISSERTATION

Scientific articles

1. Dimitrov, P. Methodological problems when using qualified electronic signature and universal two-factor authentication in web applications. Bulletin of the Union of Scientists – Varna, Ser. Economic Sciences. Science in the Service of Society: Scientific Conference of the Union of Scientists – Varna Branch, 7, 2018, 3, 287 – 293.

2. Dimitrov, P. & Petrov, P. (2025). Historiographical Study of Authentication Approaches in Computer Systems. *Izvestia Journal of the Union of Scientists - Varna. Economic Sciences Series, 14* (1) - in press.

3. Dimitrov, P. & Simeonidis, D. (2025). Security Considerations Regarding Access to Information Systems. *Izvestia Journal of the Union of Scientists - Varna. Economic Sciences Series, 14* (1) - in press.

Scientific reports

1. Dimitrov, P. Algorithmic problems in implementing two-factor authentication in web applications. Scientific Conference of Young Scientists – 2018: Proceedings, Varna: Steno, 2018, pp. 126 – 131.

2. Petrov, P., Dimitrov, P. Security Certificates in Public Web Websites of Banks from Balkan States. 9th International Conference him/her Application of Information and Communication Technology and Statistics in Economy and Education (ICAICTSEE – 2019), Oct. 24 – 26, 2019 : Conference Proceedings, Sofia : UNWE, 2019, 160 – 169.., ISSN(print) 2367-7635, ISSN(online) 2367-7643

3. Petrov, P., Buevich, A., Dimitrov, G., Kostadinova, I., Dimitrov, P. A Comparative Study him/her Web Security Technologies Used in Bulgarian and Serbian Banks. 19 International Multidisciplinary Scientific Geoconference SGEM 2019 : Conference Proceedings, 28 June – 7 July 2019, Albena, Bulgaria : Vol. 19. Informatics, Iss. 2.1, Sofia : STEF92 Technology Ltd., 2019, 3-10., ISSN(print) 13142704, ISBN(print) 978-619740876-8 / **Scopus**

4. Petrov, P., Dimitrov, P., Stoev, S., Dimitrov, G., Bulut, F. Using the Universal Two Factor Authentication Method in Web Applications by Software Emulated Device. 20th International Multidisciplinary Scientific Geoconference SGEM 2020 : Conference Proceedings, 18 – 24 Aug. 2020, Albena, Bulgaria : Vol. 20. Informatics, Geoinformatics and Remote Sensing. Iss. 2.1. Informatics, Geoinformatics, Sofia : STEF92 Technology DOI: https://doi.org/10.5593/sgem2020/2.1/s07.052, 20, 2020, 2.1, 403 – 410.., ISSN(print) 1314-2704, ISBN(print) 978-619-7603-06-4 / DOI 10.5593/sgem2020/2.1/s07.052 / **Scopus**