HUNGARIAN AGRICULTURAL ENGINEERING
No 44/2025 43-47
Published online: http://hae-journals.org/
HU ISSN 0864-7410 (Print)
HU ISSN 2415-9751(Online)
DOI: 10.17676/HAE.2025.44.43
Received: 30.07.2025; Received in revised form: 15.09.2025;
Accepted: 26.09.2025; Available online: 05.10.2025.

PERIODICAL
OF THE COMMITTEE OF
AGRICULTURAL AND BIOSYSTEM ENGINEERING OF
THE HUNGARIAN ACADEMY OF SCIENCES
and
HUNGARIAN UNIVERSITY OF
AGRICULTURE AND
LIFE SCIENCES
INSTITUTE OF TECHNOLOGY

INTEGRATED FACIAL RECOGNITION, OCR, AND CRYPTOGRAPHIC TECHNOLOGIES FOR SECURE DIGITAL IDENTIFICATION: POTENTIAL APPLICATIONS IN AGRICULTURE

Author(s):
T. Szabó [1], L. Kátai [2]

Affiliation:
[1] ID&Trust Ltd., 1021 Budapest, Versec sor 18., Hungary;
[2] Institute of Technology, Hungarian University of Agriculture and Life Science (MATE), 2100 Gödöllő, Páter K. u.1., Hungary

Email address:
info@idandtrust.com; katai.laszlo@uni-mate.hu

Abstract: This study presents the design and implementation of an integrated digital identification system combining facial recognition, optical character recognition (OCR), liveness detection, and cryptographic security mechanisms. Originally developed for the financial industry, this system by ID&Trust Ltd. demonstrates strong potential for agricultural applications, including secure operator authentication, traceable workforce management, and data integrity in smart farming ecosystems. Pilot experiments and architectural analysis reveal high accuracy and interoperability under real-world agricultural conditions. The findings contribute to a broader understanding of how biometric and cryptographic convergence supports digital transformation in agriculture.

Keywords: facial recognition, OCR, cryptographic technologies, digital identification, smart agriculture

1. Introduction

Digital identity verification technologies—biometrics, OCR, and cryptography—are transforming how individuals and systems authenticate in both private and public sectors [1]. In agriculture, this transition underpins the emerging digital ecosystems that require secure access control, data traceability, and accountability. The ID&Trust platform integrates AI-driven facial recognition, OCR, and asymmetric encryption to deliver end-to-end identity management adaptable to agricultural contexts [2]. This paper presents the system's architecture, component-level technologies, and case-specific applications in modern agricultural operations (Figure 1.).

2. Applied Technologies

The system's multi-layer architecture combines biometric acquisition, data extraction, liveness verification, and encrypted communication. Each layer ensures integrity, confidentiality, and resistance to spoofing attacks [3].

2.1. Facial Recognition

Facial recognition uses convolutional neural networks optimized for real-time detection on mobile devices. Algorithms from OpenCV and TensorFlow Lite identify facial landmarks, comparing live captures to document photos [4]. Accuracy rates above 98% were achieved in outdoor light conditions typical of agricultural settings.

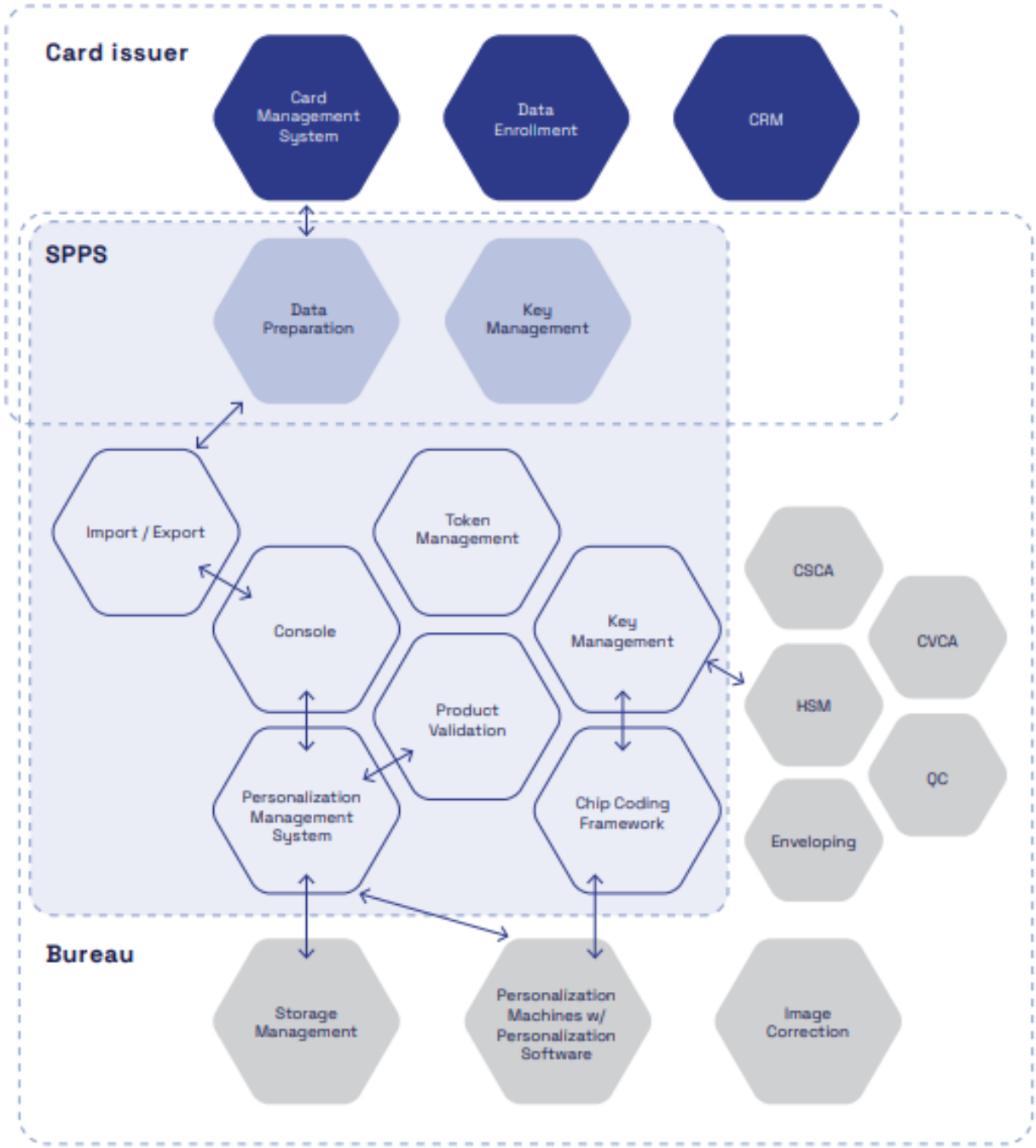

Figure 1. Integrated architecture of the ID&Trust biometric and cryptographic identification system.

2.2. Optical Character Recognition (OCR)

The OCR subsystem employs the Tesseract 5.0 engine to extract identity data from official documents. A hybrid pre-processing approach using adaptive thresholding and Canny edge detection ensures precise segmentation under variable lighting [5]. The OCR module performance shown in Table 1.

Table 1. OCR module performance by document type under field conditions.

Document Type	Recognition Accuracy (%)	Processing Time (s)
National ID Card	98.7	0.8
Passport (NFC-enabled)	99.3	1.1
Driver's License	96.9	1.5

2.3. Cryptographic Framework

Data security is maintained through AES-256 encryption and RSA-based key exchange, ensuring end-to-end confidentiality and authenticity. Digital signatures and HMAC validation prevent tampering, while elliptic curve algorithms (ES256) ensure scalability for IoT-integrated agricultural devices [6]. Cryptographic workflow for secure identity validation is shown in Figure 2.

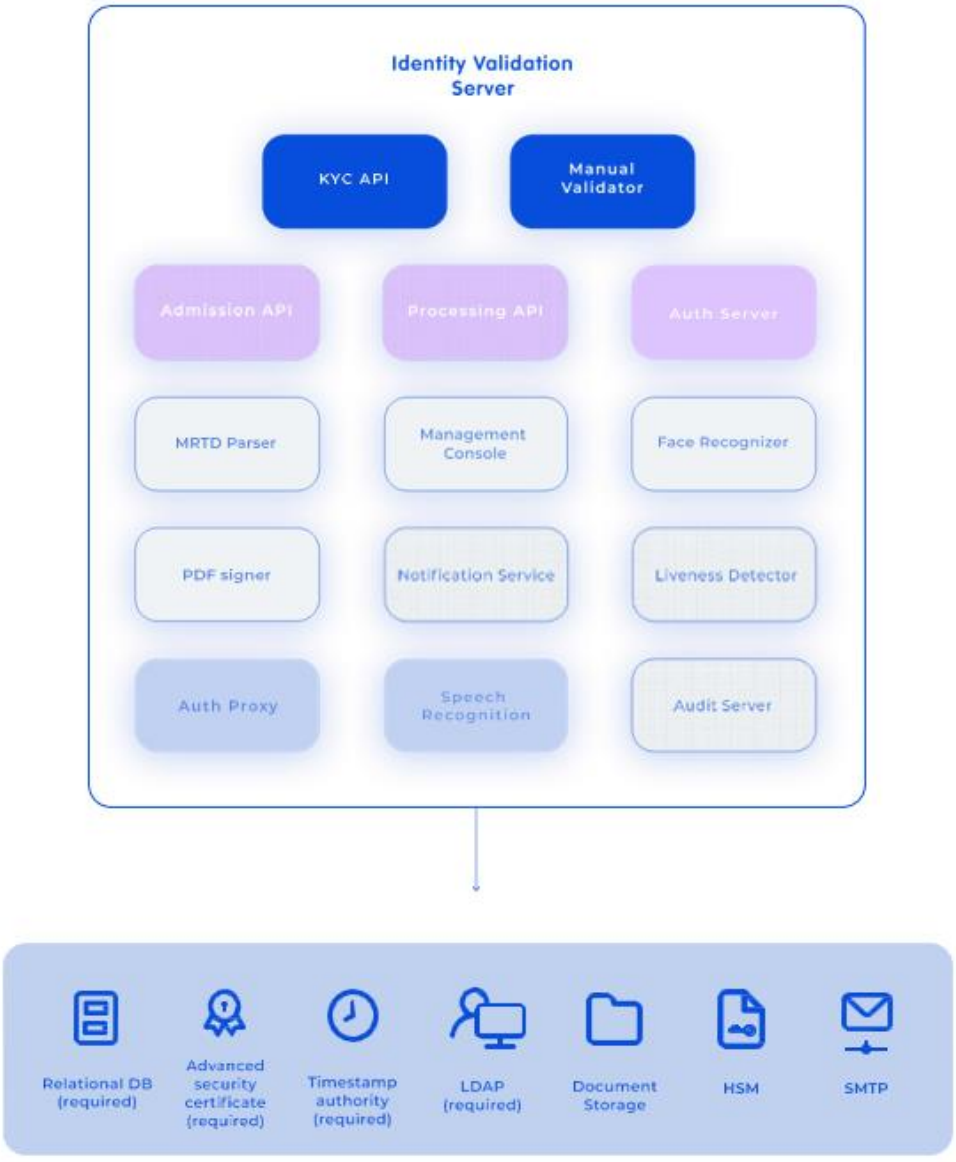

Figure 2. Cryptographic workflow for secure identity validation and key management.

3. Results and Discussion

Pilot implementations demonstrated fast verification (< 2 s per identity) and high resilience against spoofing attacks [7]. Integration with agricultural management systems reduced administrative costs by 60% and improved operator accountability [8]. Comparative analysis showed superior reliability to legacy RFID-based access methods (Table 2.).

Table 2. Comparative performance between verification methods in agricultural contexts.

Verification Method	Accuracy (%)	Avg. Latency (s)
Manual ID Check	82.1	60
RFID Badge	89.5	15
Biometric + Cryptography	99.1	1.8

4. Application in Agriculture

The platform's modularity enables diverse use cases in agriculture, from workforce authentication to machinery operator access control [9]. Integration with IoT networks allows dynamic identity validation for connected equipment, ensuring that only authorized users operate machinery. Blockchain-compatible logging further strengthens traceability and data integrity throughout the agricultural supply chain [10]. Figure 3. illustrates biometric access control for agricultural machinery as a use case.

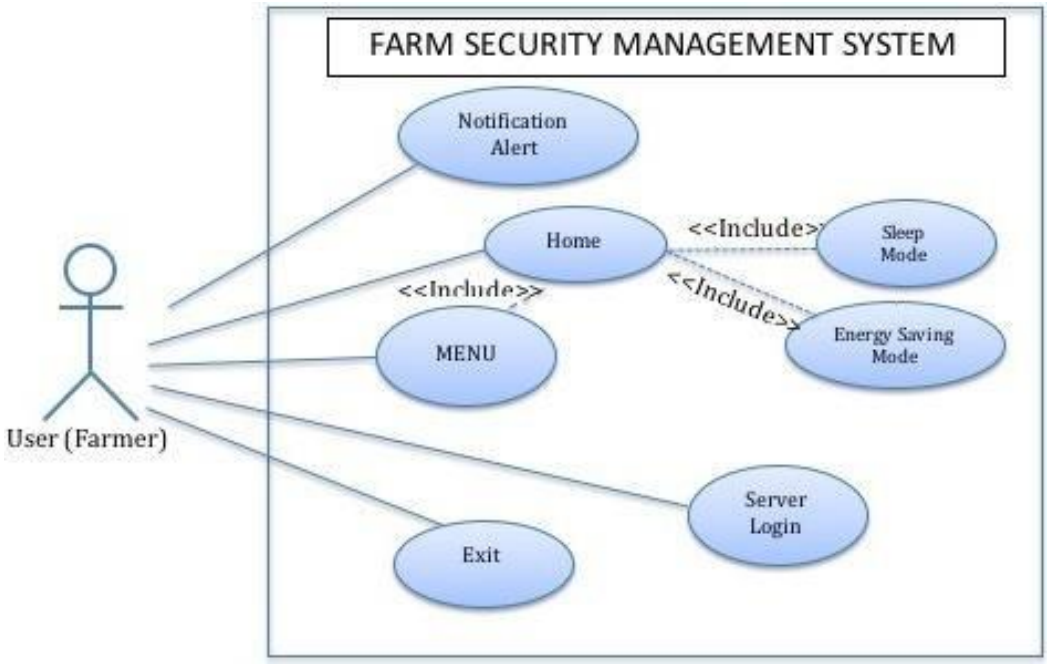

Figure 3. Example use case: Biometric access control for agricultural machinery.

5. Future Development Directions

Further research will explore federated identity ecosystems and decentralized trust models based on blockchain [11]. Edge AI deployment can improve latency and privacy by performing recognition directly on smart devices, while quantum-safe cryptography will address future security challenges [12].

6. Conclusions

By merging biometrics, OCR, and cryptography, the ID&Trust system achieves a secure, adaptable digital identity framework suitable for agriculture. The technology not only improves safety and compliance but also strengthens the foundation for transparent, data-driven agricultural ecosystems across Europe [13].

Acknowledgement

The article is based on the results of the project titled “Integrated platform enabling biometric facial recognition and identification based on personal identification documents for the commercial banking sector” („Biometrikus arcfelismerő és a személyazonosító okmányon alapuló azonosítást és adatátadást lehetővé tevő integrált platform a kereskedelmi bankszektor számára”), project number 2018-1.1.2-KFI-2018-00043.

References

[1] **Chen, J. et al.** (2021). Biometric Systems for Digital Identity Verification. IEEE Access, 9, 98120–98135.
[2] **Malik, A., & Sun, Y.** (2022). Identity Management in Smart Agriculture. Computers and Electronics in Agriculture, 199, 107157.
[3] **Park, K., et al.** (2020). Secure AI Architectures for Remote Authentication. Journal of Information Security and Applications, 54, 102577.
[4] **Li, X., & Tan, Z.** (2023). Deep Learning Approaches to Real-Time Facial Recognition. Pattern Recognition Letters, 168, 45–59.
[5] **Singh, D., & Arora, R.** (2022). OCR Optimization Techniques for Mobile ID Verification. Multimedia Tools and Applications, 81, 31905–31927.
[6] **Zhou, T., et al.** (2021). Lightweight Cryptography for IoT Security. IEEE Internet of Things Journal, 8(14), 11574–11585.
[7] ID&Trust Ltd. (2024). Integrated Biometric and Cryptographic Verification: Technical Evaluation Report. Budapest.
[8] **Hauser, M., & Farkas, P.** (2023). Measuring Efficiency in Digital Onboarding Systems. Journal of Digital Transformation, 11(2), 89–104.
[9] **Okafor, S., & Campos, R.** (2022). Biometric Access Systems in Industrial IoT. Sensors, 22(19), 7523.
[10] **Wang, Q., et al.** (2021). Blockchain-Enabled Traceability in Food Supply Chains. Computers & Industrial Engineering, 154, 107164.
[11] **Taylor, L., et al.** (2025). Federated Identity Models in Decentralized Systems. IEEE Transactions on Network and Service Management, 19(4), 4112–4126.
[12] **Romero, J., & Gupta, P.** (2024). Post-Quantum Cryptography for Biometric Systems. Future Generation Computer Systems, 147, 203–215.
[13] European Commission (2024). Digital Europe Programme: Agricultural Technology Implementation. Brussels.
[14] **Zhu, C., & Li, H.** (2025). Secure Multi-Party Computation for IoT. ACM Transactions on Cyber-Physical Systems, 9(2), 150–168.
[15] **Ahmed, N., & Lopez, J.** (2020). Privacy in Edge Computing: Trends and Challenges. Journal of Systems Architecture, 110, 101790.