ICPA
17th INTERNATIONAL CONFERENCE ON PRECISION AGRICULTURE
ConBAP 2026
CONGRESSO BRASILEIRO DE AGRICULTURA DE PRECISÃO E DIGITAL
13-16 July 2026 | Porto Alegre, Brazil
ISPA
AsBraAP

Towards Trusted Satellite Data for Precision Farming: Mitigating Spoofing and Improving Data Integrity Using Galileo OSNMA and HAS and Copernicus Traceability Service

Bram Veldhuisen[1], Joep Tummers[2], Fedde Sijbrandij[1], Trim Bresilla[1], Tamara ten Den[1], Arnab Gupta[2]

[1]Wageningen Plant Research, Wageningen, The Netherlands

[2]Wageningen Social & Economic Research, Wageningen, The Netherlands

A paper from the Proceedings of the
17th International Conference on Precision Agriculture and 11th Brazilian Congress on Precision and Digital Agriculture
13-15 July 2026
Porto Alegre, Brazil

Abstract.

Background: Precision agriculture increasingly relies on GNSS positioning not only to execute field operations with high spatial accuracy, but also to provide trustworthy data for documentation, certification, and regulatory compliance. However, GNSS signals remain vulnerable to degradation, jamming, and especially spoofing—an intentional manipulation of satellite signals causing machinery to believe it is in a different position. Such incidents have already been observed near the eastern borders of the EU, where agricultural machinery experiences sudden positional GNSS jumps that undermine both operational performance and traceability requirements. To address these vulnerabilities, the European Galileo system is introducing two complementary services: (i) the Open Service Navigation Message Authentication (OSNMA), providing cryptographic authentication of navigation messages, and (ii) the High Accuracy Service (HAS), enabling decimeter level positioning without the need for commercial RTK subscriptions. Combined with signing of the data, these services open opportunities to substantially increase trust in location-dependent processes within precision agriculture. For Earth Observation (EO) the Copernicus Data Space Ecosystem (CDSE) introduced their Traceability services which allows for the complete tracing of a data product's integrity.

Methods: This works presents the TRL 4 implementation of an authenticated agricultural machine data workflow as developed in the HASHTAG project. In the system an OSNMA and HAS capable

GNSS receiver publishes not only the standard positioning information onto the ISOBUS, but also the OSNMA and HAS status. The OSNMA and HAS status is logged as part of the as-applied data by the ISOBUS Task Controller. When this as-applied data is shown in a Farm Management Information System (FMIS), the OSNMA and HAS status are shown as extra layers, besides the commonly used data layers such as applied rate and driving speed. To prevent tampering with the data during transmission, signing of the data is implemented to ensure data integrity, authenticity, and security. This is done in all steps from requesting an EO image to the resulting as-applied map coming from the machine to the FMIS. Authenticated EO images of Copernicus are used to create task maps. For authenticating task maps and as-applied maps we propose and demonstrate a signing process. For the authentication of the data on the ISOBUS, the AEF ISOBUS Public Key Infrastructure, as used by ISOBUS TIM, can be used. This proposed solution allows for data provenance in the whole data flow.

Results: A test setup has been developed to test and demonstrate the proposed approach. In the FIMS signed task maps can be made, and data provenance of as-applied maps back to EO-images can be shown. In the field authenticity of task maps can be checked, and as-applied maps containing the OSNMA and HAS status and are signed.

Conclusion: We conclude that integrating Galileo OSNMA, HAS, and CDSE Traceability into precision agriculture data flows, together with signing of the data, can significantly improve trustworthiness in operational GNSS use, EO use and downstream accountability processes. This strengthens resilience against spoofing and enables more robust, tamper-resistant documentation for compliance, certification, and automated verification workflows.

Keywords: GNSS authentication, precision agriculture, regulatory compliance, autonomous farming, Galileo

Introduction

Precision agriculture is increasingly dependent on Global Navigation Satellite Systems (GNSS) to support both the execution and documentation of field operations. Positioning data is not only used for guidance and automation of machinery but also forms the basis for recording what has been carried out in the field, where, and at what time. This information is becoming essential for compliance with regulations, certification schemes, and the verification of agricultural practices. As a result, the role of GNSS in agriculture is shifting from a purely operational tool towards a critical component in data-driven accountability processes (Kowalczyk & Hadas, 2024; Perez-Ruiz et al., 2021).

Despite its central role, GNSS positioning in agricultural applications remains vulnerable to several limitations. Signal degradation, jamming, and spoofing can affect both the accuracy and the integrity of positioning data. Spoofing represents a growing concern, as it involves the deliberate manipulation of satellite signals, causing receivers to calculate incorrect positions without being able to detect the attack. Such incidents have been reported in regions where interference with GNSS is common, leading to sudden position shifts for agricultural machinery and undermining both operational reliability and data traceability (Gkogkos et al., 2024; Zidan et al., 2020). In parallel, the intrinsic accuracy of standalone GNSS is often insufficient for precision agriculture applications, where sub-decimeter or even centimeter-level accuracy is required. While Real-Time Kinematic (RTK) solutions can provide this accuracy, these systems depend on additional infrastructure, incur costs, and are not universally available (Pini et al., 2020).

These limitations affect not only the execution of agricultural tasks, but also the trustworthiness of the resulting data. Operation logs, also known as as-applied maps, are increasingly used as evidence in regulatory and certification contexts. However, without guarantees on positioning integrity and data authenticity, such records remain susceptible to manipulation or uncertainty. This creates a fundamental challenge: how to ensure that location-based agricultural data can be trusted as a reliable representation of what occurred in the field.

Recent developments within the European Galileo system provide new opportunities to address these issues. The Open Service Navigation Message Authentication (OSNMA) enables cryptographic authentication of GNSS signals, allowing receivers to verify that the navigation message originates from a legitimate source and has not been altered (EUSPA, n.d.-b; Hammarberg et al., 2024). In addition, the Galileo High Accuracy Service (HAS) provides corrections that enable decimeter-level positioning without the need for commercial RTK subscriptions . Together, these services offer the potential to improve both the integrity and the accuracy of GNSS-based positioning in agricultural applications (EUSPA, n.d.-a; Fernandez-Hernandez et al., 2022). At the same time, the Copernicus Data Space Ecosystem introduces traceability services that allow the origin and integrity of Earth Observation data products to be verified throughout their lifecycle (European Space Agency, n.d.).

While these technologies exist independently, they are not yet integrated into agricultural workflows. In current practice, the data flows between Earth Observation providers, Farm Management Information Systems (FMIS), and agricultural machinery are not designed to preserve and verify trust-related information across the entire chain. Furthermore, mechanisms to ensure that data remains unaltered during transmission and processing are typically lacking or only partially implemented.

The central research question addressed in this paper is therefore: how can GNSS authentication, high-accuracy positioning, and data signing be integrated into agricultural data workflows to create a verifiable and trustworthy chain from earth observation data to as-applied results?

This paper addresses this gap by presenting a TRL4 implementation of a trusted agricultural data workflow, developed within the HASHTAG project. The proposed system combines GNSS authentication and high-accuracy positioning with end-to-end data signing to establish a verifiable chain of information, from Earth Observation input to as-applied data generated by the machine. Within this workflow, GNSS receivers provide not only positioning data but also authentication and accuracy status, which is recorded as part of the operational data. In parallel, digital signatures are applied at each stage of the data flow to ensure integrity and authenticity.

The objective of this work is to demonstrate that such a trusted data chain can be realized using existing standards and prototype components under controlled laboratory conditions at TRL4. The implementation covers the full sequence of data exchange, including the creation of prescription maps based on authenticated Earth Observation data, their transformation into task maps within an FMIS, the execution of these tasks on agricultural machinery, and the generation and validation of as-applied data. Through this approach, the study demonstrates how GNSS authentication, high-accuracy positioning, cryptographic transformation, and data signing can be combined into a coherent system that supports both operational reliability and verifiable documentation.

Methods

This study presents a TRL4 implementation of a trusted agricultural data workflow in which GNSS authentication, high-accuracy positioning, and end-to-end data signing are integrated into a single data chain. The implementation follows a complete workflow from the creation of prescription data to the generation and validation of as-applied results, demonstrating how data provenance can be preserved across all stages under controlled laboratory conditions.

The overall data flow is illustrated in Figure 1, which represents the interaction between four main components: the prescription map provider, the Farm Management Information System (FMIS), the machine, and the GNSS receiver. The workflow begins with the retrieval of Earth Observation data by the prescription map provider. In this study, this role is fulfilled by the company TerraSphere, which processes Earth Observation inputs into a biomass map using the WDVI-index (Clevers, 1989). This prescription map is subsequently transferred to the FMIS, where it is first converted into a prescription map describing spatially variable application requirements and subsequently into a task map defining the intended field operation. Farmmaps is used as the FMIS system in this study.

From the FMIS, the task map is sent to the agricultural machine, where the operation is executed. During execution, the machine uses GNSS positioning data to determine its location within the field and to apply the task map accordingly. After completion of the operation, the machine generates an as-applied map that records what has been carried out, including spatially explicit application data. This as-applied map is then transferred back to the FMIS, where it can be visualized, inspected, and further processed. In this way, the workflow forms a complete chain from Earth Observation data to as-applied results.

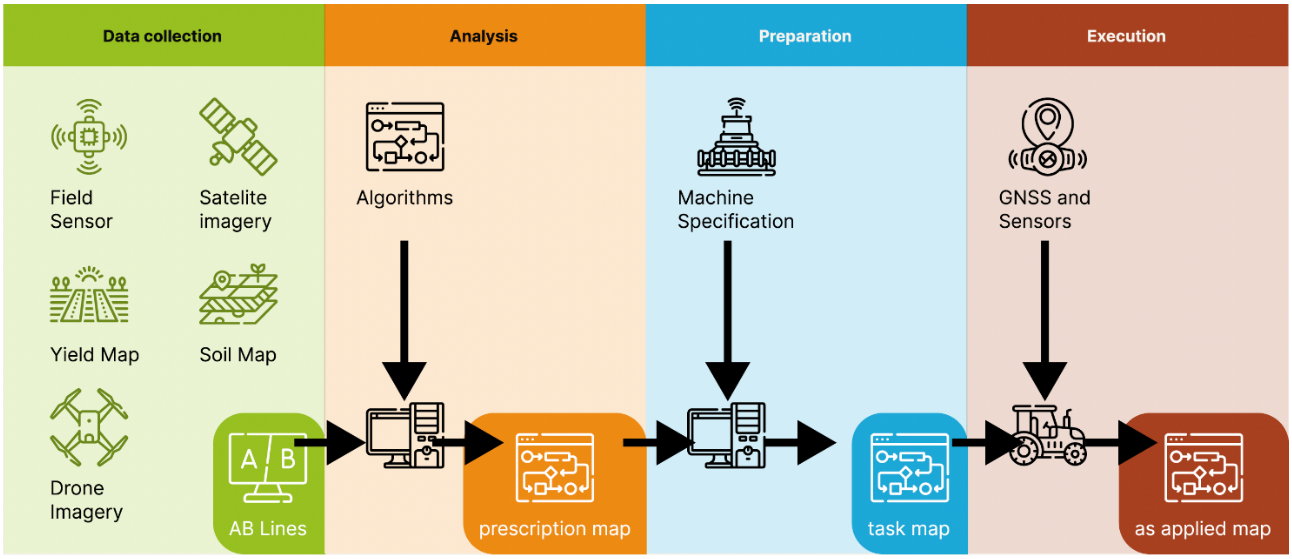

Figure 1: High level data flows in the Hashtag project. Connecting source data, prescription maps, task maps and as-applied maps into a trusted workflow (Hashtag, nd.) Licence: CC BY-CA

To ensure integrity and authenticity across this chain, a signing mechanism is applied at each stage of the workflow. Each dataset, including prescription maps, task maps, and as-applied records, is accompanied by metadata describing its contents and is digitally signed using a cryptographic key pair. This enables verification of both the origin and the integrity of the data at every step. Any modification to the data or its associated metadata results in an invalid signature, thereby providing a mechanism to detect tampering throughout the workflow.

GNSS authentication and accuracy information are incorporated at the machine level by an OSNMA- and HAS-capable GNSS receiver. In addition to standard positioning data, the receiver provides information on authentication status and positioning quality. This information is made available within the machine environment and recorded as part of the as-applied data. As a result, each recorded position is associated with explicit indicators of its trustworthiness and accuracy, allowing these attributes to be analyzed and visualized within the FMIS alongside conventional operational data layers.

The implementation was realized in a laboratory test setup, shown in Figure 2, which reproduces the essential components of the machine–FMIS data chain. The setup consists of a commercial ISOBUS terminal (CCI1200), an implement Electronic Control Unit (EPEC EC44) emulating a field implement, and a workstation acting as a prototype control unit responsible for handling GNSS-related data and message exchange. A GNSS simulator was used to provide controlled and repeatable positioning inputs, including variations in authentication status, enabling systematic testing without the need for field deployment.

Within this setup, the ISOBUS Task Controller executes the task maps received from the FMIS and logs operational data, including GNSS position and associated trust information, into an as-applied file. The resulting datasets are exported from the machine and processed on a separate pc where signing and validation steps are performed. The FMIS is used to generate task maps from prescription data and to visualize the resulting as-applied data, including the recorded GNSS authentication and accuracy indicators.

The validation of the system focuses on three aspects. First, the robustness of the signing mechanism is assessed by verifying that any modification to data or metadata leads to invalidation of the signature. Second, the propagation of GNSS authentication and accuracy information is evaluated by confirming that these attributes are consistently captured and preserved in the as-applied data. Third, the functionality of the validation process is tested by applying it to correctly signed datasets as well as intentionally modified data. Together, these steps provide evidence of the system's ability to maintain and verify data provenance across the full workflow.

The implemented system represents a laboratory-scale integration of the proposed data flow and does not yet constitute a fully integrated operational environment. Data exchange between components is partially performed through manual steps, and signing and validation are not yet embedded within all system components. In addition, the use of a GNSS simulator instead of a physical receiver and the absence of a production-level certificate infrastructure reflect the TRL4 nature of the implementation. These limitations are addressed further in the Discussion section.

Figure 2: Test set-up. With CCI1200 terminal on the left. The WUR PC behind the CCI1200, the EPEC EC44 lays behind the CCI1200. The screen is connected to the WUR PC, the GNSS simulator on the right of the image

Results

The implemented workflow was validated using a laboratory test setup in which the complete data chain from task map generation to as-applied data validation was executed. The results focus on three key aspects: the integrity of the signing mechanism, the propagation of GNSS trust information, and the functionality of the validation workflow.

The execution of the workflow on the machine side confirmed that all relevant components were correctly connected and operational. As shown in Figure 3, both the implement (sprayer) and the HASHTAG electronic control unit (ECU) were recognized by the CCI1200 terminal, indicating that the ISOBUS network was correctly configured and that the additional GNSS-related functionality was successfully integrated into the machine environment. During operation, GNSS data and associated HASHTAG status messages were received and processed by the terminal, as illustrated in Figure 4, where the incoming HASHTAG message is visible on the interface.

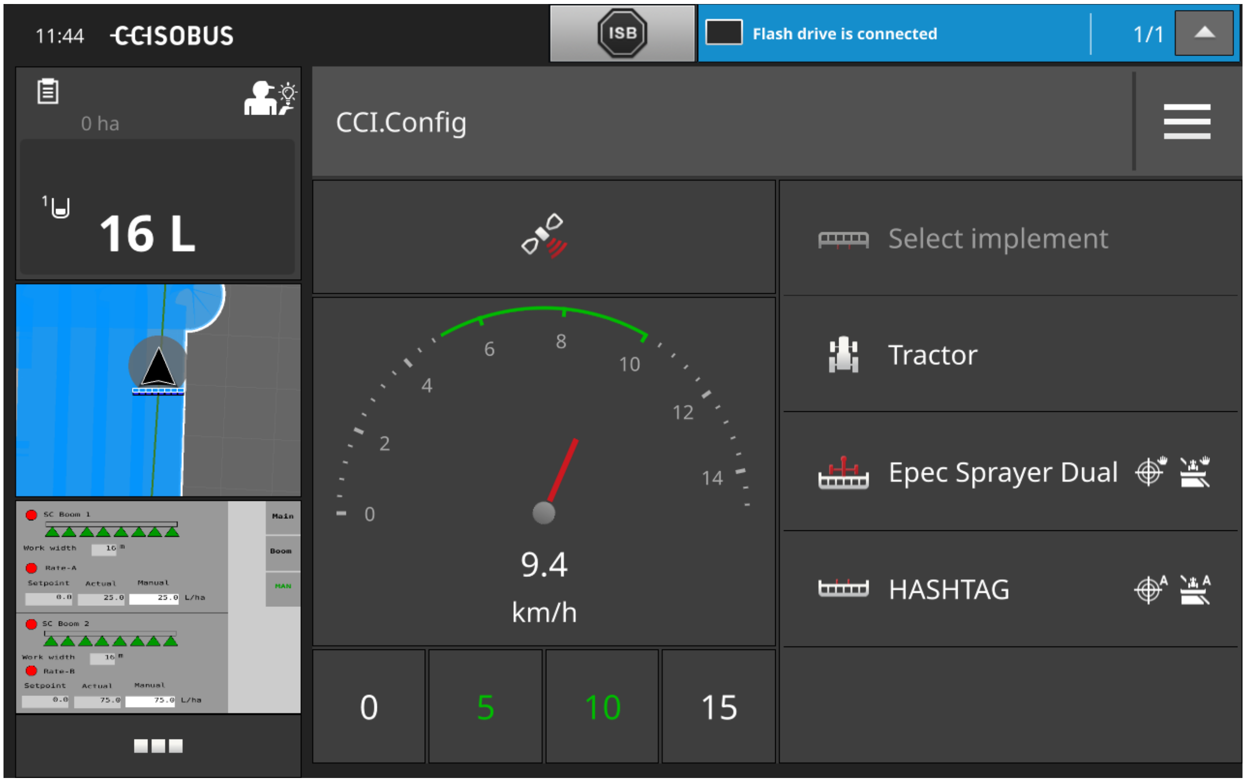

Figure 3: Screenshot of CCI1200. Both the Sprayer and the Hashtag ECU are connected to the terminal

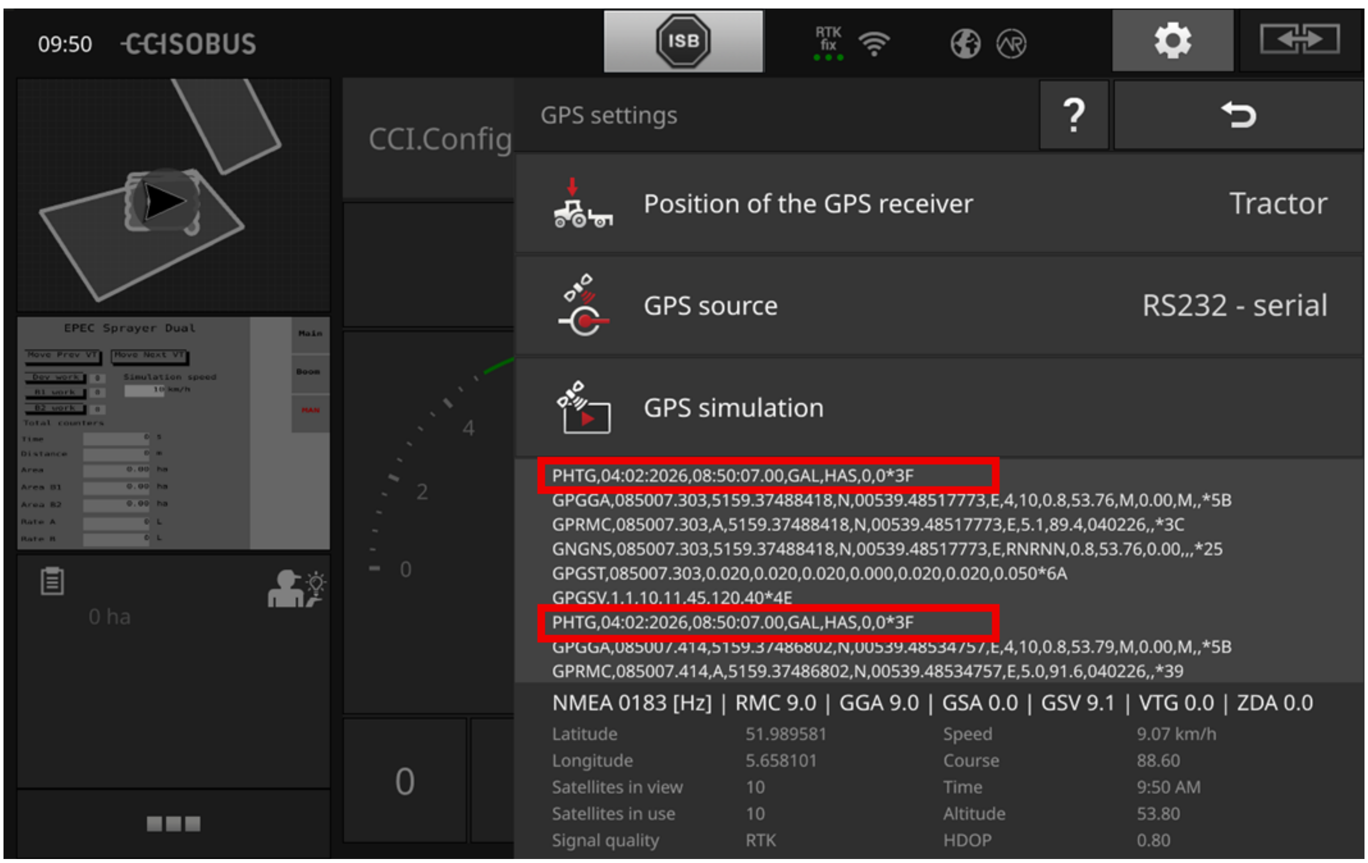

Figure 4: Screenshot of CCI1200 terminal. Received HASHTAG Message circled in red

The second result relates to the integration and propagation of GNSS authentication and accuracy information within the data flow. During execution of the task map, the GNSS receiver provided both positioning data and associated trust indicators derived from OSNMA and HAS status. These indicators were successfully transmitted within the machine environment and recorded as part of the as-applied dataset. When processed in the FMIS, these trust indicators could be visualized alongside standard operational data layers. An example of this visualization is shown in Figure 5, where the HAS status is represented spatially, allowing a direct assessment of the trustworthiness of positioning data used during the field operation. This confirms that GNSS trust information is preserved throughout the workflow and remains accessible for interpretation at the FMIS level.

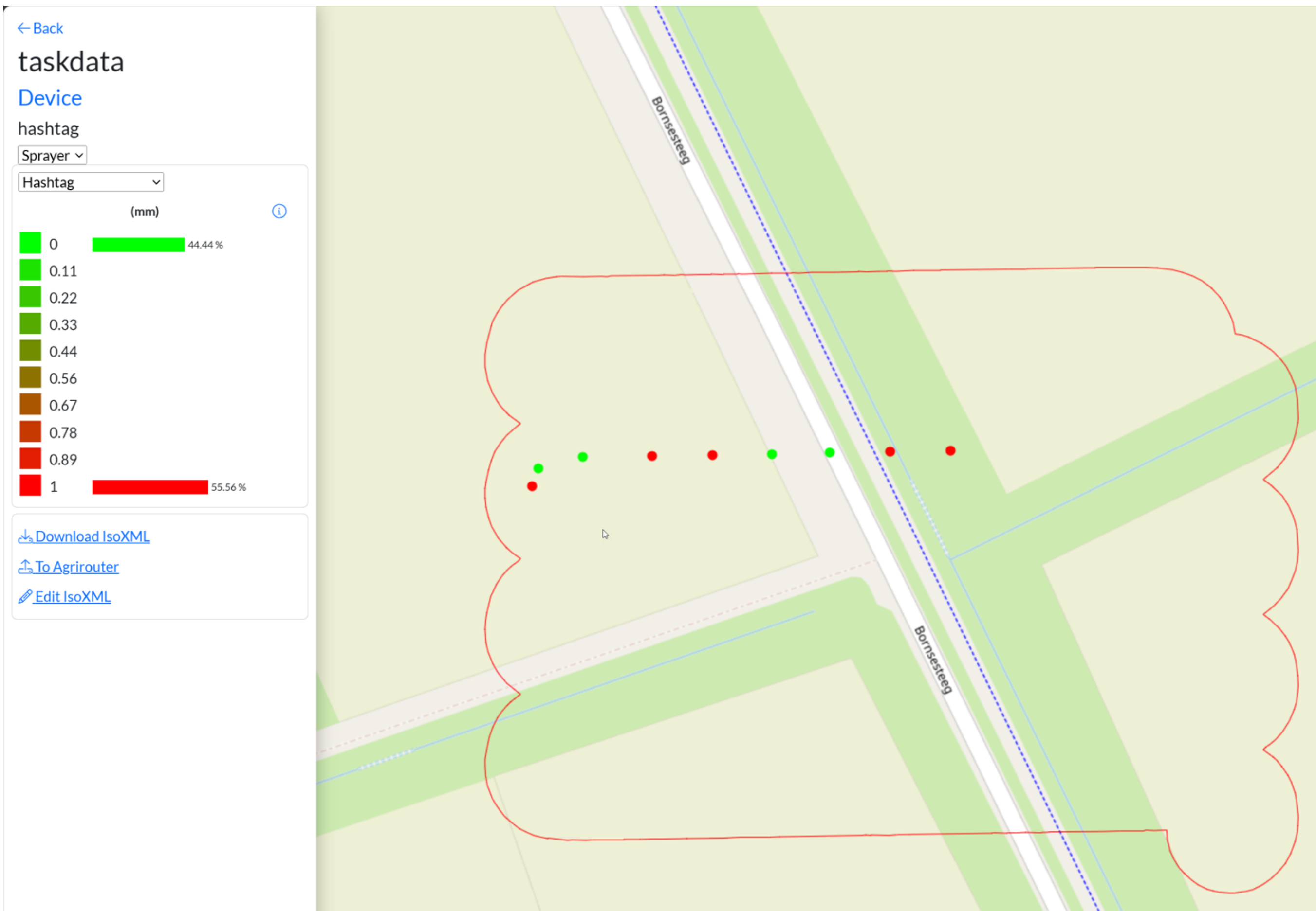

Figure 5: Visualization of Hashtag status in FMIS (FarmMaps). 1= HAS status confirmed, 0 = HAS status not confirmed

The third result concerns the robustness of the digital signing mechanism. An open source signing and validation tool, developed within the HASHTAG project and made available via GitHub (Hashtag, 2026/2026), was used to sign and verify all datasets exchanged within the workflow. Validation tests showed that any modification to the data, including small changes to the ISOXML content or alterations to associated metadata, resulted in an invalid signature. This behavior was consistent for both task maps and as-applied datasets, demonstrating that the applied signing method provides a reliable mechanism for ensuring data integrity across the entire workflow.

The functionality of the validation process was further demonstrated by testing different data conditions. Correctly signed datasets were successfully verified using the appropriate public key, while validation failed when data had been altered. Figure 6 shows an example in which a minor modification was introduced into the task data within a compressed archive. The validation tool correctly detected the inconsistency and reported the dataset as invalid. Similar behavior was observed for modifications to metadata, indicating that both data content and associated descriptive information are protected by the signing framework.

In addition to these core results, the tests confirmed that the full data chain from FMIS to machine and back to FMIS could be executed within the laboratory setup. Task maps generated in the FMIS were successfully executed on the machine, and the resulting as-applied maps were returned and processed further. While some steps in this process required manual intervention, such as file transfer and signing operations, the overall data flow remained intact and traceable. Together, these results demonstrate that the proposed approach enables a verifiable chain of data in which both the integrity of the data and the trustworthiness of the underlying GNSS positioning can be assessed.

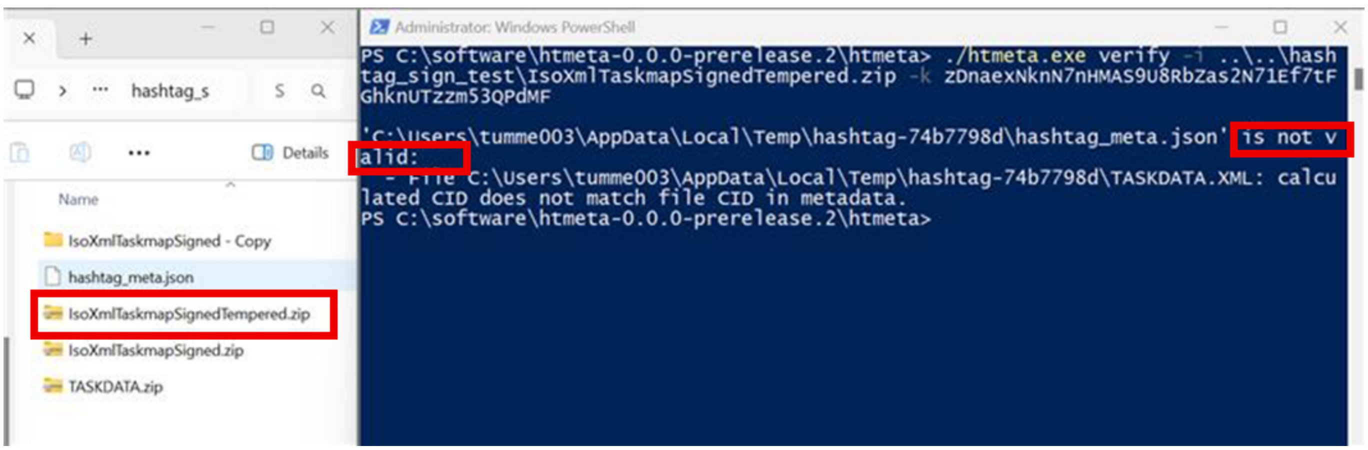

Figure 6: Validation of a zip file in which there was tampered with the coordinates in the task data

Discussion

The results of this study demonstrate that a trusted agricultural data workflow, combining GNSS authentication, high-accuracy positioning, and end-to-end data signing, can be realized within a controlled laboratory environment. The implementation shows that it is technically feasible to establish a verifiable chain from taskmap data to as-applied results, in which both the integrity of the data and the trustworthiness of the underlying positioning information can be assessed. At the same time, the findings also highlight several limitations and challenges that must be addressed before such a system can be applied in operational agricultural settings.

A key outcome of this work is the confirmation that digital signing provides a robust mechanism for protecting data integrity across the workflow. The validation results show that even minimal modifications to either data content or metadata are reliably detected, ensuring that tampering cannot go unnoticed. This is particularly relevant in the context of agricultural compliance and certification, where as-applied data is increasingly used as supporting evidence. However, while the cryptographic mechanisms themselves are effective, their practical implementation introduces complexity. In the current setup, signing and validation are performed using external tooling rather than being embedded within operational systems such as the FMIS or machine terminal. As a result, the workflow still relies on manual steps, which limit its usability and scalability in real-world applications.

A second finding is that GNSS authentication and accuracy information can be successfully integrated into the machine data flow and preserved throughout the workflow. In the TRL4 level setup this information is added as proprietary data to the as-applied map. For further implementation it will need to be added to the standard. The inclusion of OSNMA and HAS status in the as-applied dataset enables a direct link between operational data and the quality of the underlying positioning. This represents a significant step towards improving trust in GNSS-based agricultural data, particularly in environments where spoofing or signal degradation may occur. At the same time, it should be noted that the current work focuses on the propagation and recording of this information, rather than on evaluating the performance of OSNMA or HAS themselves. In particular, the high-accuracy positioning capabilities enabled by HAS were not independently quantified in this study and rely on results reported elsewhere (EU Agency for the Space Programme, n.d.).

The laboratory-based nature of the implementation represents an important limitation of the present work. The system was validated at TRL4 using a desk setup and a GNSS simulator, which allowed controlled and repeatable testing of the data flow. While this approach is appropriate for demonstrating technical feasibility, it does not capture the full complexity of real-world field conditions. For example, the system was not tested under actual GNSS interference scenarios such as spoofing or jamming, as these cannot be reproduced in operational environments due to regulatory constraints. In addition, the use of a simulator instead of a physical GNSS receiver means that further validation is needed to confirm behavior under real signal conditions.

Another limitation relates to the degree of system integration achieved in the current implementation. The data flow between components is not yet fully automated, and several steps, including data transfer and signing, are performed manually. Furthermore, commercial machine terminals, such as the CCI1200 used in this study, do not natively support the processing or validation of HASHTAG metadata and signatures. As a result, trust assessment is currently performed at system level rather than directly on the machine. This reflects a broader challenge in the agricultural technology landscape, where proprietary systems limit the integration of new data standards and functionalities.

Beyond technical integration, the results highlight the need for a broader governance framework to support trusted data exchange. While digital signatures allow verification that data has not been altered and that it originates from a specific source, they do not by themselves establish whether that source is trusted. In the current implementation, cryptographic keys are generated and exchanged locally, without the involvement of a trusted certificate authority. For large-scale deployment, this approach is insufficient. A robust Public Key Infrastructure (PKI), such as the one developed by the Agricultural Industry Electronics Foundation (AEF), is required to ensure that identities can be verified consistently across systems. Establishing such a trust framework is essential for enabling interoperability and for ensuring that validation results can be interpreted in a meaningful and consistent way.

The findings of this study also have implications for the standardization of agricultural data flows. Existing standards such as ISOBUS and ISOXML provide a solid foundation for interoperability, but do not yet fully support the integration of GNSS authentication data or digital signatures. The current implementation therefore relies on extensions and external metadata structures to preserve this information. For wider adoption, these concepts need to be formalized within standardized data models and communication protocols. At the same time, care must be taken to ensure that such extensions remain compatible with existing systems and do not introduce unnecessary complexity.

Taken together, the results show that the main challenge in enabling trusted agricultural data workflows is no longer the availability of the underlying technologies, but their integration into existing systems and practices. GNSS authentication, high-accuracy positioning, and digital signing are all available, but have not yet been combined into a coherent, operational workflow. The present study demonstrates a first step towards such integration at TRL4, indicating that a fully functional and user-friendly implementation is achievable. Future work should therefore focus on system-level integration, automation of data exchange and validation processes, and validation under real-world field conditions, to move from prototype implementation towards practical deployment. Several functionalities are still being further developed within the project, including tools to show the signing status in the FMIS interface. Furthermore in-field tests are planned to help improve transparency and usability

Conclusion

This study demonstrates that a trusted agricultural data workflow, combining GNSS authentication, high-accuracy positioning, and end-to-end data signing, can be implemented under controlled laboratory conditions at TRL4. The results show that data integrity can be reliably ensured through digital signatures, that GNSS trust information can be preserved within as-applied datasets, and that validation processes can effectively detect any data manipulation.

By integrating Galileo OSNMA and HAS with signing mechanisms and traceability concepts, the proposed approach enables a verifiable chain from prescription data to as-applied results. This provides a foundation for improving the trustworthiness of agricultural data, particularly in applications related to compliance, certification, and accountability.

Although further work is required to achieve full system integration and validation under field conditions, the findings indicate that the proposed approach offers a technically viable pathway towards secure, tamper-resistant, and trustworthy data exchange in precision agriculture.

Acknowledgments

This work was supported by the European Union through the European Union Agency for the Space Programme project HASHTAG under Grant Agreement No. 101180.

AI Statement

The authors used generative artificial intelligence tools (Microsoft Copilot Enterprise) for language refinement, proofreading, and improving the clarity and readability of the manuscript.

References

Clevers, J. G. P. W. (1989). Application of a weighted infrared-red vegetation index for estimating leaf area index by correcting for soil moisture. Remote Sensing of Environment, 29(1), 25-37.

EU Agency for the Space Programme. (n.d.). *Galileo HAS ready to increase efficiency of farming tasks. Latest tests prove suitability for precision agriculture* |. Retrieved May 27, 2026, from https://www.euspa.europa.eu/newsroom-events/news/galileo-has-ready-increase-efficiency-farming-tasks-latest-tests-prove

European Space Agency. (n.d.). *Copernicus Data Space Ecosystem*. Retrieved May 27, 2026, from https://documentation.dataspace.copernicus.eu/

EUSPA. (n.d.-a). *Galileo HAS in force Reference Documents | European GNSS Service Centre (GSC)*. Retrieved May 27, 2026, from https://www.gsc-europa.eu/electronic-library/programme-reference-documents/galileo-in-force/has

EUSPA. (n.d.-b). *Galileo OSNMA in force Reference Documents | European GNSS Service Centre (GSC)*. Retrieved May 27, 2026, from https://www.gsc-europa.eu/electronic-library/programme-reference-documents/galileo-in-force/osnma

Fernandez-Hernandez, I., Chamorro-Moreno, A., Cancela-Diaz, S., Calle-Calle, J. D., Zoccarato, P., Blonski, D., Senni, T., de Blas, F. J., Hernández, C., Simón, J., & others. (2022). Galileo high accuracy service: Initial definition and performance. *GPS Solutions*, *26*(3), 65.

Gkogkos, D.-E., Mamatas, L., & Petridou, S. (2024). Assessing supervised machine learning in detecting GPS spoofing attacks on UAV application use-cases. *2024 27th Conference on Innovation in Clouds, Internet and Networks (ICIN)*, 138–142.

HASHTAG. (n.d.). HASHTAG — Harmonised Standards for Trusted Agricultural Data Flows. Retrieved June 5th, from https://hashtag-project.eu/

Hammarberg, T., García, J. M. V., Alanko, J. N., & Bhuiyan, M. Z. H. (2024). An experimental performance assessment of Galileo OSNMA. *Sensors*, *24*(2), 404.

Hashtag. (2026). *Hashtag-eu/hashtag-meta* [C#]. hashtag-eu. https://github.com/hashtag-eu/hashtag-meta (Original work published 2026)

HASHTAG. (n.d.). HASHTAG — Harmonised Standards for Trusted Agricultural Data Flows. Retrieved June 5th, from https://hashtag-project.eu/

Kowalczyk, W. Z., & Hadas, T. (2024). A comparative analysis of the performance of various GNSS positioning concepts dedicated to precision agriculture. *Reports on Geodesy and Geoinformatics*, *117*.

Perez-Ruiz, M., Martínez-Guanter, J., & Upadhyaya, S. K. (2021). High-precision GNSS for agricultural operations. In *GPS and GNSS Technology in Geosciences* (pp. 299–335). Elsevier.

Pini, M., Marucco, G., Falco, G., Nicola, M., & De Wilde, W. (2020). Experimental testbed and methodology for the assessment of RTK GNSS receivers used in precision agriculture. *IEEE Access*, *8*, 14690–14703.

Zidan, J., Adegoke, E. I., Kampert, E., Birrell, S. A., Ford, C. R., & Higgins, M. D. (2020). GNSS vulnerabilities and existing solutions: A review of the literature. *IEEE Access*, *9*, 153960–153976.