RFID-assisted Continuous User Authentication for IoT-based Smart Farming

Alexander Bothe, Jan Bauer, Nils Aschenbruck

University of Osnabrück, Institute of Computer Science
Wachsbleiche 27, 49076 Osnabrück, Germany
Email: {bothe, bauer, aschenbruck}@uos.de

***Abstract*—Smart Farming is driven by the emergence of precise positioning systems and Internet of Things technologies which have already enabled site-specific applications, sustainable resource management, and interconnected machinery. Nowadays, so-called Farm Management Information Systems (FMISs) enable farm-internal interconnection of agricultural machines and implements and, thereby, allow in-field data exchange and the orchestration of collaborative agricultural processes. Machine data is often directly logged during task execution. Moreover, interconnection of farms, agricultural contractors, and marketplaces ease the collaboration. However, current FMISs lack in security and particularly in user authentication. In this paper, we present a security architecture for a decentralized, manufacturer-independent, and open-source FMIS. Special attention is turned on the Radio Frequency Identification (RFID)-based continuous user authentication which greatly improves security and credibility of automated documentation, while at the same time preserves usability in practice.**

***Index Terms*—RFID; NFC; Security; Authentication; Smart Farming**

I. Introduction & Motivation

Leveraged by modern information technology and Internet of Things (IoT) concepts, the primary sector of economy is changing. In this context, Smart Farming enables resource efficiency and yield optimization, while having the potential to increase sustainability [4], [12]. A crucial component of smart farming is the so-called Farm Management Information System (FMIS) that allows an optimal overview on available resources, an efficient management, and the control of farm equipment. Furthermore, FMISs also ease the provision of services and provide automatic documentation [5], [7], [9].

In the present agricultural practice, there is a infrastructure of historically grown software solutions for FMISs on the one hand, and for additional sections of the value chain on the other hand, ranging from logistics systems over telemetry systems to proprietary software of contractors. However, this infrastructure is very heterogeneous, and therefore interoperation is not always possible. The missing interoperability hinders a collaboration between all actors. In this context, the project open software platform for service innovation in a value added network for agriculture (ODiL) develops an open and decentralized platform for agriculture services. Amongst others, the goal of ODiL is data sovereignty since there is often a conflict with data owners' intention when using existing software systems in current practice. For example, when farmers cooperate with contractors, agricultural machinery manufacturers, and service providers, sensitive business data inevitably leaves the farm. Although ODiL involves all actors of value chains and provides global functionality as marketplaces and interest groups, the focus of this paper is on its FMIS component. For an adequate orchestration of cooperative vehicles in harvesting scenarios, for instance, ODiL's FMIS facilitates the farm-internal management of inventory, the control of field operations, and the interconnection of machinery. Moreover, also the integration of novel IoT technologies that already reached the market, such as shed and storage monitoring, are possible, similar to the future integration of Wireless Sensor Networks [10] or drone-based field monitoring, e.g., [12].

Finally, for traceability, the FMIS provides an automatic documentation of processes. Particularly for that purpose, the registration of responsible employees is mandatory and, thus, their authentication is necessary. However, security is neglected in agricultural practice as the absence in current surveys (cf. [5]) and a view into existing FMIS products reveal. Despite of being briefly mentioned in reference architectures in the literature (e.g., [7], [9]), available FMIS products do not yet fully support user authentication and authorization.

In this paper, we present a comprehensive security architecture for the ODiL platform covering confidential communication between individual actors and an authorization framework that ensures data sovereignty. For a required hardware initialization of different components in this platform, we introduce an easy to use RFID-based approach. Moreover, by using ODiL's FMIS as a representative system, we propose a cost-efficient and feasible approach for a continuous RFID-based user authentication that is exemplarily evaluated to authenticate users on agricultural machines and greatly supports traceability within FMISs.

The remainder of the paper is organized as follows: The next section contains a short overview of ODiL's framework and terminology. Then, the underlying security architecture is introduced (Sec. III), focusing on confidential communication and authorization. In Section IV, special attention is given to the user authentication in the driver's cabin of an agricultural machine including a comparison of various applicable technologies. Section V presents the implementation and results, whereas Section VI finally concludes the paper.

DOI: 10.1109/RFID-TA.2019.8892140

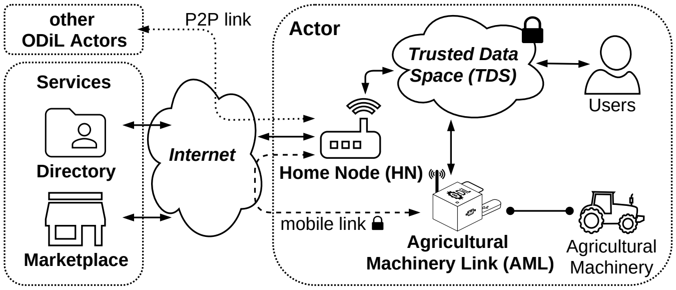

Fig. 1. Overview on the overall ODiL framework, its interconnection of agricultural actors, and secured communication channels.

II. ODiL Background

Decentralization is crucial for establishing an open service delivery network in agriculture. It enables an equal participation and supports the sovereignty business and personal data. Therefore, ODiL is designed as an open and decentral framework consisting of self-sufficient networks, as visualized in Figure 1. Such networks correspond to farms, contractors, or other actors of the agricultural value chain, such as machinery rings, seed and fertilizer producers, and processing industries.

In a farm network, for instance, all the resources of a company (e.g., machines, employees, and storages) are connected with a farm server. Those servers, called Home Nodes (HNs) in the context of ODiL, handle the entire farm-internal data management and provide an API for Representational State Transfer (REST) communication. By using cryptography and a strict access control, they form a Trusted Data Space (TDS) for connected resources, cf. Fig. 1. Moreover, a Graphical User Interface (GUI) provides various user groups with functionality to gather, process, visualize, and (knowingly) share farm data with other users or ODiL actors.

Cross-company cooperation is realized by an infrastructure that enables actors to purposefully share services, requests, and data. To this end, it provides a central directory, marketplaces, and also automatically generated interest groups. The directory is used for the registration of HN networks which is important for our security architecture and provides a name resolution service (comparable to the Domain Name System (DNS)). Via marketplaces, the actors can offer or request agricultural services, machinery, and products. For the sake of privacy, offers and requests are separated into public and private components and only the former are publicly available in the marketplaces. If mutually interested, actors are introduced to each other and share private components using Peer-to-Peer (P2P) communication, i.e., directly and not through a third-party instance.

The vertical integration up to machine level is achieved by a specific hardware accessory, called Agricultural Machinery Link (AML) which is compatible with existing machines and extends the terminal in the vehicles driver cabin, using a connection to the machine's Controller Area Network (CAN) (ISO 11898). In this way, the AML can act as a gateway between the embedded CAN and the corresponding HN network. It delivers ISOBUS[1] data (ISO 11783) from the machine to the HN and vice versa, cf. Fig. 1. Note that not all ISOBUS data is necessarily relevant for the FMIS. Furthermore, some data might be sensitive from a privacy perspective, e.g., if it contains user-specific information. Thus, it is also a task of the gateway to filter this kind of information. A privacy-aware approach for such a filtering has been recently introduced in [1]. For the HN connection, either WLAN is used if the machine is in range of an access point of its HN's TDS, or Public Land Mobile Networks (PLMN) communication. In both cases, the Message Queue Telemetry Transport (MQTT) protocol, a modern message-based IoT standard, is used and parametrized for a reliable PLMN data delivery of mainly periodical sensor data streams in rural areas [2].

III. Security Architecture

The primary security goal of ODiL is the data sovereignty of individual actors which is crucial to protect both business related as well as personal data. The design of ODiL's security architecture essentially relies on two well-known and practically proven security standards. First, as basic technique to secure both a confidential communication and the integrity of exchanged data, the Transport Layer Security (TLS) protocol[2] is used. Secondly, we take advantage of OAuth2[3], a modern authorization framework and open standard which enables a powerful and flexible approach to purposively limit the access to sensitive resources. The extension of the general framework with both security protocols is briefly introduced in the following subsections.

A. Home Node Registration & Public Key Infrastructure

In the framework of ODiL, TLS can be used globally, i.e., for HN to infrastructure and P2P communication between individual HNs, and locally within a particular HN network. Here, TLS not only secures the TDS but also each TCP/IP connection that is established via PLMNs, cf. Fig. 1. TLS typically relies on a trusted Public Key Infrastructure (PKI). We realized such a PKI by extending the directory with PKI capabilities. For that purpose, we implemented both a Certificate Authority (CA) and an Registration Authority (RA) component with corresponding REST services. The CA root certificate has to be preinstalled in each HN, and thus is integrated into its source code.

The entire certificate creation process is integrated into the HN's initial setup procedure. It is inspired by common practices of account creation for Internet services with an increased security demand such as online banking. Figure 2 gives an overview on this process. In the first phase, the owner of an HN initiates the registration process. Using a web-interface, he signs up to the ODiL platform by transmitting his name along with an email and postal address to the RA of the directory. Note that this initial communication is already TLS encrypted, enabled by the preinstalled CA root certificate. For a validation check, the RA replies with a confirmation link

[1] https://www.isobus.net/isobus/

[2] RFC 5246, https://tools.ietf.org/html/rfc5246

[3] RFC 6749, https://tools.ietf.org/html/rfc6749

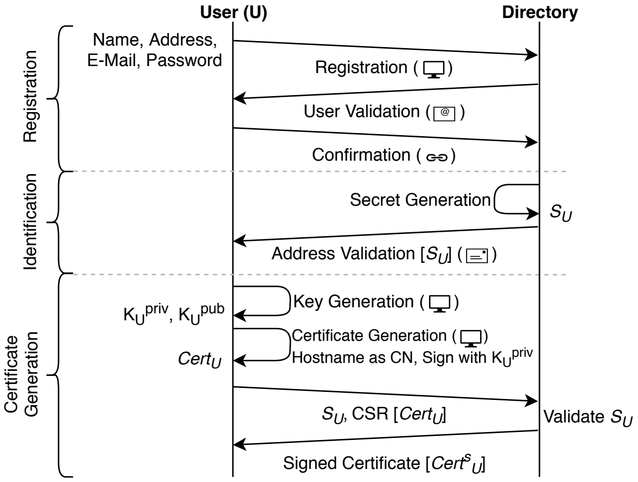

Fig. 2. Account creation and certificate signing process diagram.

which is finally confirmed by the owner. In the next phase, a specific secret S_U (e.g., a password) is generated by the directory and sent to the given address by mail in order to verify the HN's identity. After receiving this secret, the HN generates a cryptographic key pair, i.e., a public K_U^{pub} and a private K_U^{priv} key. It then generates an X.509 certificate $Cert_U$ using its hostname as Common Name (CN) which is subsequently signed with its private key. Then, a Certificate Signing Request (CSR) is sent to the CA that includes the secret which is entered by the owner. In case, the secret is valid, i.e., it corresponds to the provided account, and the sender address (hostname) also matches the CN included in the CSR, the CA finally replies to the CSR with a signed certificate $Cert_U^S$ that is afterwards used for the internal TDS and for external P2P communication with other HNs.

B. Authorization Framework

ODiL aims at a user-centric approach, which allows individual actors to explicitly control the access rights of all entities within their TDS. Using a Role-based Access Control (RAC), the access to farm resources, machinery, and employee data can be configured. Thereby, the owner of an HN can also define where business and personal data is stored and at which point in time which information is shared with other actors in the global network. Hence, ODiL offers a selective visibility of data which is highly demanded by the community.

ODiL's RAC enables a dynamic and GUI-assisted configuration of individual users, their roles, and associated access rights inside the TDS. As already mentioned, we use OAuth2 to realize this access control. Therefore, each HN is extended by an OAuth authorization server. After a specific configuration, the set of RAC rules is mapped to so-called OAuth scopes and delivered to this server. Whenever access to a certain resource is requested by a user, he firstly has to contact this server in order to request a bearer token. In case, access is permitted, i.e., the request is included in the corresponding scopes of the user, such a token is granted. Subsequently, this token can be used for both, the REST and MQTT communication within the TDS. On the HN side, each resource server receiving a token is now able to permit or deny the access based on the validation results of the token, using the corresponding service of the authorization server.

For the MQTT-based communication, a special plugin for the Eclipse Mosquitto[4] broker was developed and successfully established in the ODiL framework. Exploiting the user name field in the header of a (TLS encrypted) MQTT message for the token, OAuth is seamlessly integrated into existing MQTT components. A specific token manager in the plugin is responsible for the validation and also for possible refreshes of the token. Mosquitto already has an Access Control List (ACL) feature. However, this ACL is static because it is only initialized once when the broker is started. For this reason, a dynamic ACL was implemented that is continuously reconfigured by the token manager during the broker's execution.

As mentioned in the previous section, TLS enables a secure communication but, because only server-side certificates are used, it does not ensure the authentication of communicating clients. However, when issuing a token, OAuth also checks the authenticity of individual entities via user credentials prior to the authorization. Thus, additional TLS certificates for users would be redundant, and besides, would significantly complicate the maintenance and, thus, decrease the usability. Note that, in addition to the user credentials, there are also client credentials that are integrated into certain OAuth flows to validate the authenticity and authority of all communicating entities, such as the AML which is used by a machine driver. For details on the extensive OAuth framework, refer to the corresponding RFC[3].

IV. Continuous User Authentication

The user acceptance and lastly the success of the holistic ODiL framework strongly depends on the security and the privacy offered. However, an increased system security usually has a detrimental effect on the usability, which has to be minimized by selecting appropriate mechanisms.

Without loss of generality, we focus on the user authentication in the driver's cabin of an agricultural machine, enabling user authorization and automated process documentation. Although a user-layout data mask is already specified, user management is not included in the corresponding standard (ISO 11783-6) and, thus, not implemented in existing terminals. Therefore, to the best of our knowledge, it is generally not provided by available commercial FMISs.

During daily use, the expected security threats are mainly limited to carefree usage, e.g., forgotten logouts and weak or lost credentials. Nevertheless, a malicious user might try to compromise the system using various, universal attacks (cf. [6], [8]). For this paper, we limit our evaluation to whether it is possible to remotely eavesdrop on the authentication process or to gain unauthorized access to the (stored) credentials, both enabling further attacks (e.g., cloning) on the system. Without loss of generality, we assume the AML to be

[4] https://mosquitto.org

a trusted and secure device. In addition to security aspects, scenario-related environmental factors like dust, humidity, and vibrations caused by the machine must also be taken into account. Furthermore, the costs and longevity have an influence on the acceptance of the system.

In the ODiL framework, a feasible and cost-efficient user authentication is realized on the AMLs (cf. Fig. 1). For this purpose, two requirements must be met: First, the AML has to integrate the user authentication mechanism into the OAuth authorization framework (cf. Sec. III-B). Leveraging that OAuth tokens with a relatively short lifetime decrease the potential for misuse, a continuous user authentication scheme is used, frequently polling the user's credentials. Secondly, to establish a continuous connection between HN and AML, initially individual configuration data has to be transferred, including the HN's identifier, login details for the TDS, and the AML's OAuth client credentials. Depending on the selected user authentication mechanism, additional information (e.g., passwords, fingerprints) may need to be transferred.

In the consecutive subsections, various authentication techniques will be briefly described and evaluated in context of the designated scenario. In addition, we will assess whether they can be leveraged for the initial data transfer.

A. Conventional & Biometric Authentication

The most common method for user authentication is manual input of individual credentials. Consisting of a user identifier and password or Personal Identification Number (PIN), they can be entered via keyboard, touch or PIN pad. In this case, initialization data has to be transferred manually by the user as well.

The security level of this method usually varies with both, strength and length of the credentials and discretion of individual users. Given these points, as long as the users remember their credentials, this method is relatively secure. Yet, for the designated scenario it is not feasible, as due to the continuous authorization requirement, the driver would be distracted from the actual task. In addition, the input device might be susceptible to dust/humidity (affecting longevity) and vibrations caused by the machine might be detrimental to the input process. The overall cost is strongly related to the robustness of the selected interface.

To avoid the need to memorize credentials, biometric identification can be used. For this purpose, several fingerprint sensors are available. Their capturing process can be based on various types of biometric sensors, whereas optical or capacitive sensors are commonly used. For identification, the scanned fingerprint is processed and matched to stored templates which have to be generated and distributed to all relevant readers at an initial stage (enrollment). In addition, they have to be kept up to date and a mapping from the matching template to the user's credentials has to be provided. Moreover, alternative communication methods are needed to transfer initialization data to the AMLs.

Even though fingerprints provide a relatively high level of security and are generally invariant on a long-term perspective, this method of authentication is again not feasible for the designated scenario, as most of the practical issues from using manual input remain. Furthermore, additional privacy concerns arise in handling fingerprint data of employees.

Face recognition, another option utilizing biometric identification features, can be implemented based on a camera attached to the AML. The required facial features can then be extracted from both, fixed-images and videos. Similar to fingerprints, templates for comparison have to be generated in a prior step and need to be linked to user credentials. From a long-term perspective either regular updates or an age invariant face recognition algorithm might be required. Furthermore, the camera can be used to transfer initialization data, e.g., by using QR codes displayed on the HN's GUI.

Theoretically, this method is applicable to the agricultural scenario described, as the driver can be authenticated continuously without distraction. As long as the underlying algorithm recognizes and ignores fake images, face recognition provides a good level of security. In practice, the feasibility is strongly related to the conditions in the drivers cabin: Again, dust, humidity and vibrations may have an impact on the success rate of the authentication process. In addition, the lighting conditions in the cabin and the camera angle in relation to the driver, can be a detrimental factor. However, due to the used camera, which could be misused to constantly monitor employees, serious privacy concerns arise.

B. Universal Serial Bus (USB)

A regular USB storage device can not only be used for (initial) data transfer, but also for authentication. The users credentials are first written to the device by the HN and later, while plugged in, continuously polled and used by the AML.

In general, USB devices are a valid option to be used for AML user authentication. In regards of longevity, they usually can retain data for multiple years, and are mainly limited by the number of write operations. As user credentials usually are comparably small, cost efficient low memory sticks are feasible. Nevertheless, there are several downsides of this mechanism: Apart from very specialized devices, no inherent cross platform compatible access control and encryption standard exists. Even using third party encryption, the technique remains susceptible to cloning attacks, due to the lack of access control mechanisms. Secondly, dust, humidity caused corrosion, vibrations, and mechanical stress from the attachment/detachment process can lead to issues with the connection or the device's electrical circuit.

C. Bluetooth Low Energy (BLE)

In general, contactless alternatives can be used to improve overall robustness (e.g., less exposed hardware interfaces) and usability of the authentication process. Both Bluetooth and BLE can be used for regular data transfer, whereby in particular the latter, in the form of BLE beacons which periodically and actively broadcast their identifier, is already utilized in agricultural context. An FMIS using this technology, though not for authentication, is the 365Acitve system[5]: A tablet installed in each driver cabin scans for nearby BLE beacons, which are, e.g., handed out to employees, or attached to agricultural machines and implements. Using the provided app, previously registered beacons in the vicinity can be selected and assigned to a task.

From a security perspective, we do not advise to use BLE beacons as a user authentication method. The main drawback is, that BLE beacons always broadcast their identifier to all receivers in range without encryption. Thus, an eavesdropped message can either be replayed to gain access, or used to create a cloned beacon. The longevity of the system is determined by the beacon's battery lifetime, which depends on the set transmission strength and interval. For the 365Active system it is estimated, that the battery has to be replaced approx. every 4 years.

D. Radio Frequency Identification (RFID)

Due to its inherent advantages, e.g., no line-of-sight requirement, resistance against various environmental influences, and batch reading capabilities, RFID is already frequently used in Smart Farming and corresponding logistics [11]. However, to the best of our knowledge, to date it is not used for user authentication in this context. Without loss of generality, we focus on RFID based technologies working at high (13.56 MHz) and ultra high frequencies (860–960 MHz).

The general standard for item management using High Frequency (HF) RFID (ISO 18000-3) specifies three application depended modes: (1) Card reading; (2) Bulk reading of multiple HF tags; (3) Item management based on the EPC HF protocol. There are two main standards regarding card reading: ISO 14443 defines the general requirements and transmission protocols for proximity cards, whereas ISO 15693 (incorporated in the first mode of ISO 18000-6) specifies protocols for vicinity cards, which can operate at a longer range. Furthermore, additional card types (e.g., JIS 6319-4 FeliCa) and (proprietary) protocols exists. To communicate between two near field coupled devices, the ISO 18092 standard (Near-Field Communication (NFC)), extends the ISO 14443 standard to add card emulation and P2P communication. The required formats and protocols are defined by the NFC Forum: For information storage and exchange between suitable NFC devices, the NFC Data Exchange Format (NDEF) is used. To enable P2P communication, the Logical Link Control Protocol (LLCP) specifies the basics for bi-directional communication between NFC devices, e.g., used by the stateless request/response Simple NDEF Exchange Protocol (SNEP) for data exchange. Furthermore, tags which offer an additional I²C interface for data access from the AML exist.

Compared to HF based solutions, Ultra High Frequency (UHF) RFID can provide a significantly extended read range. The most prominent protocol for communication between interrogators and tags is specified in the EPC C1 G2 standard, which is incorporated into ISO 18000-6C and offers basic security features. Starting from the second version (ISO 18000-63), multiple security features, e.g., allowing (mutual) authorization between tags and readers and encrypted communication, have been introduced. Typically UHF RFID does neither support tag emulation, nor P2P communication between devices. To exchange initialization data either an intermediate tag (preferably with I²C interface) has to be used, or a standard conform tag emulation could be implemented, e.g., using software defined radio (cf. [3]).

In general, user authentication methods based on passive RFID are preferable for the designated scenario. From a security point of view, various options exist to secure the user credentials from the considered attack vectors, especially if instead of using the tag identifier, the credentials are stored in the tags' user memory. The level of security strongly depends on the tag chosen, as security features range from simple password based access (susceptible to eavesdropping) to non proprietary standard (e.g., Advanced Encryption Standard (AES)) based access and encrypted communication. In regards to longevity, RFID tags can offer data retention times of approx. 10 years. As passive tags are used, no battery changes are required. Furthermore, due to its wireless nature, both tags and reader can be protected from environmental influences.

V. Implementation & Evaluation

The advantages and disadvantages of the authentication techniques presented in the previous section are supplemented and summarized in Table I. On the one hand, the selected techniques are compared from an economical and a technological perspective, particularly with respect to security issues. On the other hand, usability considerations and robustness issues are listed, based on our experiences from several field tests.

Due to a high level of security combined with cost efficiency, we decided to implement an NFC based user authentication for the ODiL framework. Currently, NXP NTAG based cards are used which offer password based access control, but no transmission encryption. They are scheduled to be replaced by cards based on recent NXP DESFire chips, which offer a higher level of security (e.g., AES). For simple testing without requiring specialized hardware, we alternatively implemented the USB variant, regardless of the mentioned security concerns (cf. Sec. IV-B and Tab. I). Furthermore, both solutions have the advantage that the initial transfer of configuration data (cf. Sec. IV) can be realized in a convenient manner.

Our prototypical AML implementation is based on a Raspberry Pi 3B, with a custom designed case, as shown in Figure 3. For user authentication, an NXP PN532 based HF/NFC reader has been integrated. In addition, a LTE modem with an external antenna is used to establish the PLMN based connection to the authorization service of the HN. To provide optical and acoustical user feedback, an LED and a beeper have been added, indicating the current authentication status. The additional CAN interface, enabling data exchange between the machine's network and the HN (cf. Sec. II), is realized by a PiCAN 2 board (SK Pang Electronics). Position or speed information available via this interface might in addition

[5] https://www.365farmnet.com/en/product/365active-system

TABLE I
EVALUATION OF USER AUTHENTICATION TECHNIQUES.

			Biometric		Token-based			
		Manual Input	Fingerprint	Face Recog.	USB Dongle	BLE Beacon	NFC	UHF
Usability	User involvement	–	–	+	○	+	○	+
	Cost efficiency	–/+	–/+	–/+	+/–	+/–	+/○	–/○
	Longevity	–/+	–/+	+/○	–	+/○	+/+	+/+
	Privacy	+	○	–	+	+	+	+
Security	Eavesdropping	–	+	○	+	–	+	+
	Protected Credentials	+*	○	○	–	–	+	+
Robustness	Dust/Humidity	○/+	–/○	–/+	–	+/○	+/+	+/+
	Vibration	–	–	–	○	+	+	+

Two values in a cell represent estimates for interrogator/credentials. Marked cells indicate our main criterion for exclusion. *If not written down.

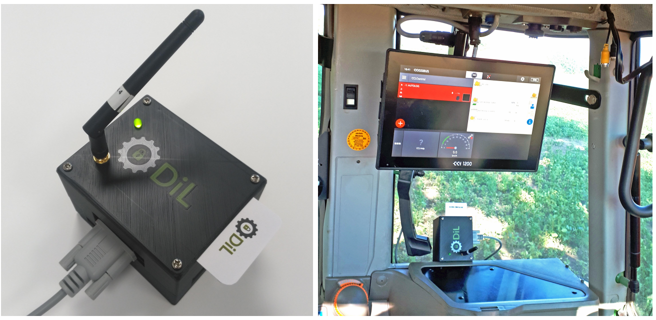

Fig. 3. Prototypical realization of the developed AML using NFC cards for a continuous user authentication on agricultural machines.

be leveraged to increase the usability of the authentication process, e.g., by reminding the user to remove his card in case the machine has stopped or left the field.

VI. CONCLUSION

In this paper, we have introduced a general architecture for a decentralized, open service delivery system in agricultural scenarios, with special emphasis on both security and data sovereignty, using well established technologies.

To secure communication channels, both globally and in the independent, self-sufficient actor networks, TLS is utilized, based on certificates issued by a PKI integrated in the systems service infrastructure. In addition, OAuth2 is used to implement a user-friendly RAC mechanism for both users and devices. As it has not been implemented in existing FMIS solutions and machine terminals, special emphasis is placed on the user authentication on agricultural machinery. After evaluating and comparing various potential mechanisms, due to the special requirements in the given scenario, an HF RFID based solution was selected, prototypically implemented, and evaluated in field tests. While ensuring usability, this solution greatly improves security and enables traceability in agricultural practice.

For future work, we would like to go beyond exemplary studies and deploy the system to a network of multiple, full-fledged and interacting agricultural businesses. This would allow us to gain deeper insight into the overall acceptance of the system and to further improve it with regard to special or everyday needs.

ACKNOWLEDGMENTS

The authors would like to thank Thomas Hänel and René Helmke for substantial implementation support.

This work is part of the ODiL project (https://www.odil-projekt.de/flyer). It was partially funded by the German Federal Ministry of Education and Research (BMBF) within the Program "Innovations for Tomorrow's Production, Services, and Work" (02K14A194). The authors are responsible for the contents of this publication.

REFERENCES

[1] J. Bauer, R. Helmke, A. Bothe, and N. Aschenbruck, "CAN't track us: Adaptable Privacy for ISOBUS Controller Area Networks," *Comput. Stand. Inter.*, vol. 66, p. 103344, 2019.

[2] J. Bauer and N. Aschenbruck, "Measuring and Adapting MQTT in Cellular Networks for Collaborative Smart Farming," in *Proc. of IEEE Conference on Local Computer Networks (LCN)*, Singapore, 2017, pp. 294–302.

[3] A. Briand, B. B. Albert, and E. C. Gurjao, "Complete Software Defined RFID System Using GNU Radio," in *Proc. of the IEEE Conference on RFID-Technologies and Applications (RFID-TA)*, 2012, pp. 287–291.

[4] S. Cox, "Information technology: the global key to precision agriculture and sustainability," *Comput. Electron. Agr.*, vol. 36, no. 2–3, pp. 93–111, 2002.

[5] S. Fountas, G. Carli, C. Sørensen, Z. Tsiropoulos, C. Cavalaris, A. Vatsanidou, B. Liakos, M. Canavari, J. Wiebensohn, and B. Tisserye, "Farm management information systems: Current situation and future perspectives," *Comput. Electron. Agr.*, vol. 115, pp. 40 – 50, 2015.

[6] A. Khattab, Z. Jeddi, E. Amini, and M. Bayoumi, *RFID Security*. Springer Berlin Heidelberg, 11 2017, ch. RFID Security Threats and Basic Solutions, pp. 27–41.

[7] J. Kruize, J. Wolfert, H. Scholten, C. Verdouw, A. Kassahun, and A. Beulens, "A reference architecture for Farm Software Ecosystems," *Comput. Electron. Agr.*, vol. 125, pp. 12 – 28, 2016.

[8] A. Mitrokotsa, M. R. Rieback, and A. S. Tanenbaum, "Classifying RFID attacks and defenses," *Information Systems Frontiers*, vol. 12, no. 5, pp. 491–505, Nov 2010.

[9] R. Nikkilä, I. Seilonen, and K. Koskinen, "Software architecture for farm management information systems in precision agriculture," *Comput. Electron. Agr.*, vol. 70, no. 2, pp. 328 – 336, 2010, special issue on Information and Communication Technologies in Bio and Earth Sciences.

[10] A.-u. Rehman, A. Z. Abbasi, N. Islam, and Z. A. Shaikh, "A Review of Wireless Sensors and Networks' Applications in Agriculture," *Comput. Stand. Inter.*, vol. 36, no. 2, pp. 263–270, 2014.

[11] L. Ruiz-Garcia and L. Lunadei, "The role of RFID in agriculture: Applications, limitations and challenges," *Comput. Electron. Agr.*, vol. 79, no. 1, pp. 42 – 50, 2011.

[12] D. Vasisht, Z. Kapetanovic, J.-h. Won, X. Jin, R. Chandra, A. Kapoor, S. N. Sinha, M. Sudarshan, and S. Stratman, "Farmbeats: An IoT Platform for Data-driven Agriculture," in *Proc. of USENIX Conference on Networked Systems Design and Implementation (NSDI)*, Boston, MA, USA, 2017, pp. 515–528.