A. Ruckelshausen et al. (Hrsg.): Digitale Marktplätze und Plattformen,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2018 243

Leichtgewichtige Infrastruktur zur Schaffung von Sicherheit und Vertrauen in einem digitalen Ökosystem für Agrardaten

Sven Wagner[1], Andrea Horch[2], Bernard Kilian[3] und Heiko Roßnagel[4]

Abstract: Bei der Digitalisierung landwirtschaftlicher Prozesse sowie der Prozesse in der Lieferkette werden Daten aus sehr unterschiedlichen Datenquellen generiert und verarbeitet. Zur Schaffung von Sicherheit und Vertrauen ist eine Verifizierung der Datenquellen erforderlich. Der hier entwickelte Ansatz erzielt dies durch ein leichtgewichtiges Identitäts- und Zugriffsmanagement, wobei auf die existierende und global verfügbare Infrastruktur und Sicherheitsstandards des Domain Name System (DNS) aufgebaut wird. Weitere Merkmale der Infrastruktur sind eine Kombination aus dezentralen Zugriffskontrolllisten und zentraler Zugriffsrechtevergabe. Das digitale Ökosystem für Agrardaten wird exemplarisch für einen Verbund mehrerer Landwirte dargestellt. Weitere mögliche Anwendungsszenarien werden aufgezeigt. Die Infrastruktur zeichnet sich durch ein hohes Maß an Flexibilität, eine gute Skalierbarkeit sowie ein weltweites Einsatzgebiet im Bereich Agrarbusiness aus.

Keywords: Datensicherheit, Identitätsmanagement, Zugriffsmanagement, Sensordatennetzwerk, vertrauenswürdiges Ökosystem.

1 Einleitung

Zur Steigerung der Effizienz in landwirtschaftlichen Betrieben sowie der Lieferkette der landwirtschaftlichen Erzeugnisse, werden die damit verbundenen Prozesse digitalisiert, um ein automatisiertes Monitoring zu ermöglichen. Herausforderungen hierbei sind insbesondere die Heterogenität der Daten, die z.B. über intelligente Sensortechniken gesammelt werden, wie auch die Gewährleistung der Datensicherheit und des Datenschutzes. Die Daten werden normalerweise an einer Stelle gespeichert und verarbeitet oder über Datenschnittstellen zusammengeführt. Hierbei müssen die Authentizität und die Integrität der Daten sichergestellt werden, wofür eine entsprechende Infrastruktur bereitgestellt werden muss. Dieser Beitrag beschreibt die Entwicklung eines vertrauenswürdigen Ökosystems für Agrardaten, das die Datensicherheit gewährleistet. Hierbei wird auf Arbeiten des Fraunhofer IAO im Rahmen der Projekte *LIGHTest* und *Industrial Data Space* und der darin entwickelten Ansätze zur Gewährleitung der Sicherheit und Vertrauenswürdigkeit der Daten zurückgegriffen und auf die Anforderungen von Agrardaten erweitert.

[1] Universität Stuttgart, IAT, Allmandring 35, 70569 Stuttgart, {firstname.name}@iat.uni-stuttgart.de
[2] Fraunhofer IAO, Identity Management, Nobelstr. 12, 70569 Stuttgart, {firstname.name}@iao.fraunhofer.de
[3] INCAE Business School, n La Garita, Alajuela, 960-4050, Costa Rica, {firstname.name}@incae.edu
[4] Fraunhofer IAO, Identity Management, Nobelstr. 12, 70569 Stuttgart, {firstname.name}@iao.fraunhofer.de

2 Verwandte Arbeiten

In den letzten Jahren wurden zahlreiche Datenplattformen und *Data Hubs* für Agrardaten entwickelt, z.B. die *GODAN* Initiative [GO17] mit dem Ziel weltweiter und frei verfügbarer landwirtschaftlicher und ernährungsrelevanter Daten und darauf aufbauender Systeme. Des Weiteren sind im Bereich *Smart Farming* zahlreiche Anwendungen entwickelt worden, z.B. im EU Projekt *Smart Agri-Food* [SA17] oder die Produkte von *Smart Farm Systems Inc.* [SF17]. Im Rahmen des *LIGHTest* Projekts [LI17] wird eine globale, domänenübergreifende Vertrauensinfrastruktur entwickelt, bei der unabhängige Behörden Vertrauensinformationen basierend auf der bestehenden Infrastruktur des Internet *Domain Name System* (DNS) veröffentlichen können. Im *Industrial Data Space* [ID17] soll ein virtueller Datenraum geschaffen werden, der einen sicheren Austausch und eine einfache Verknüpfung von Daten in Geschäftsökosystemen erleichtert. Ein Referenz-*Use Case* ist hierbei *end-to-end sensors*.

3 Leichtgewichtiges Identitäts- und Zugriffsmanagement

Die hier vorgestellte Infrastruktur zeichnet sich durch zwei zentrale Merkmale aus: Erstens, wird eine Kombination aus dezentralen Zugriffskontrolllisten und zentraler Zugriffsrechtevergabe verwendet. Zweitens, wird auf die existierende und global verfügbare Infrastruktur und Sicherheitsstandards des DNS [Mo83a], [Mo83b] und den mit Sicherheitsmechanismen erweiterten DNSSEC aufgebaut. Dabei kann u.a. auf den existierenden, globalen Vertrauensanker von DNS zurückgegriffen werden.

Als Beispiel für die hier vorgestellte, leichtgewichtige Infrastruktur in einem digitalen Ökosystem für Agrardaten, ist in Abbildung 1 exemplarisch ein Verbund mehrerer Landwirte dargestellt. In jedem Betrieb werden Sensoren eingesetzt, z.B. für das Monitoring des Bodens und der Pflanzen, für den Düngemittel- und Bewässerungseinsatz, bei Landmaschinen, etc. Hierbei erstellt und pflegt jeder Betrieb eine Zugriffsliste von seinem Sensornetzwerk. Diese beinhaltet Informationen zu den installierten Sensoren und deren Zertifikaten. Des Weiteren können IP-Adressen von Empfängern, z.B. Landwirte, Maschinenpark, Logistikpartner hinzugefügt werden. Zusätzlich werden häufig noch frei verfügbare Daten aus dem WWW (z.B. Wetterdaten) in die Entscheidungsprozesse mit einbezogen. Für das leichtgewichtige Identitäts- und Zugriffsmanagement wird ein Zugriffsmanager, ein zentraler DNS Server mit DNSSEC Erweiterung sowie ein Dokument, das die Zugriffsregelung enthält, benötigt. Hierbei fungiert der Zugriffsmanager als Kontrollinstrument, das die Weiterverarbeitung der empfangenen Sensordaten regelt. Der zentrale DNS-Server enthält die Liste aller vertrauenswürdiger Sensoren der im Ökosystem beteiligten Landwirte, die kontinuierlich hinsichtlich Änderungen in den dezentralen Zugriffslisten (z.B. neue Sensoren) aktualisiert wird. Die für jeden Sensor dazugehörigen *Resource Records* im DNS beinhalten den Sensornamen, den Fingerabdruck des Zertifikats, sowie den Zeiger auf die dazugehörige dezentrale Zugriffsliste.

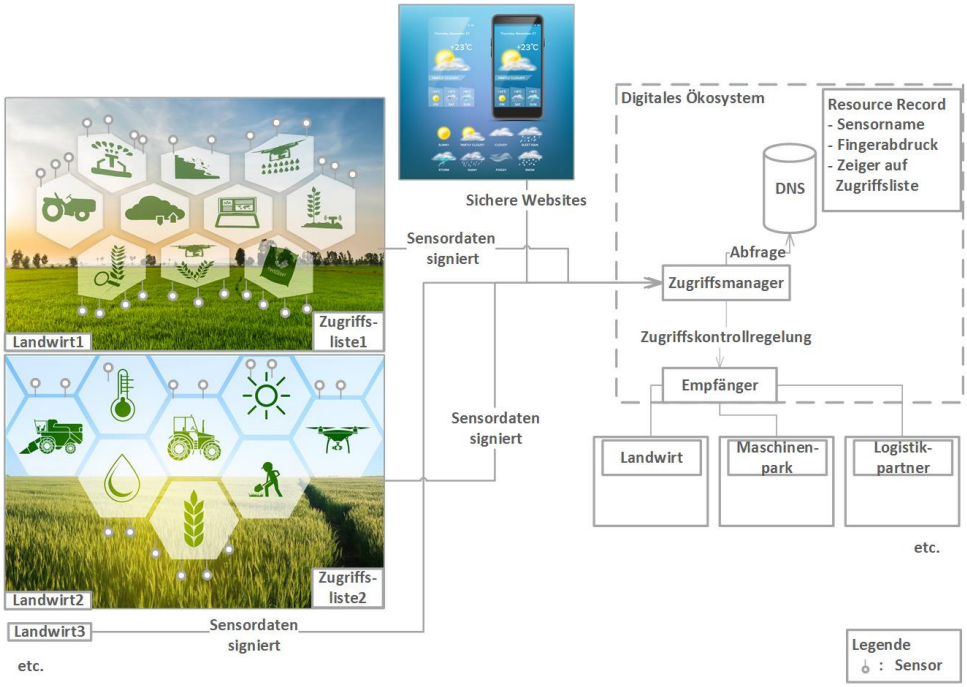

Abb. 1: Schema des leichtgewichtigen Identitäts- und Zugriffsmanagement für ein digitales Ökosystem für Agrardaten

Das zentrale Dokument mit den Zugriffsregelungen im digitalen Ökosystem ermöglicht für jeden Sensor und für jeden Landwirt spezifische Zugriffskontrollregeln zu definieren, die bei dem Entscheidungsprozess mitberücksichtigt werden müssen. Im einfachsten Fall wird angenommen, dass der Identität des Sensors vertraut wird, wenn dieser in der Liste im zentralen DNS-Server aufgeführt ist und dass die Sensordaten an einen oder mehrere Empfänger weitergeleitet werden.

Das Ablaufschema für eingehende Sensordaten, die von einem vertrauenswürdigen Sensor stammen, ist wie folgt: Die Sensordaten senden in definierten Intervallen die Messdaten an das digitale Ökosystem. Diese werden auf Authentizität und Integrität geprüft. Hierfür führt der Zugriffsmanager eine Abfrage beim zentralen DNS Server des digitalen Ökosystems durch und verifiziert den Namen und das Zertifikat des Sensors mit den vom DNS Server enthaltenen Informationen zu Sensorname und Fingerabdruck des Zertifikats. Des Weiteren ermöglicht der Zugriffsmanager die Weitergabe der Sensordaten an entsprechende Kontaktpersonen. Hierfür fragt der Zugriffsmanager die dazugehörige dezentrale Zugriffsliste des Sensors ab und erhält weitere Informationen, z.B. die IP-Adresse von Kontaktpersonen. Im letzten Schritt, wird die für jeden Sensor definierte Zugriffskontrollregelung angewendet und überprüft, ob die Identität des Sensors vertrauenswürdig ist.

Falls dies der Fall ist, werden die relevanten Informationen an die Empfängerliste weitergegeben. Zusätzlich zu dem in Abbildung 1 gezeigten Verbund mehrerer Landwirte kann z.B. noch die Lieferkette der landwirtschaftlichen Erzeugnisse in einem oder mehreren Modulen mit jeweils eigenen Zugriffslisten mit aufgenommen werden.

4 Anwendungsszenario

Die Anwendbarkeit des entwickelten Identitäts- und Zugriffsmanagements soll in Zukunft am Beispiel von Kleinbauern in Costa Rica für Kaffee- und Früchteanbau aufgezeigt werden. Aktuell werden beispielsweise sehr große Datenmengen in Bezug auf die Erfüllung von Umweltauflagen und Nachhaltigkeitsstandards erhoben, die auch für die verschiedenen Teilnehmer der Wertschöpfungskette, wie z.B. Exporteure und Handel, von Bedeutung sind. Ein weiterer Anwendungsbereich ist mit Hilfe eines Monitoringsystems unterstützt durch Fernerkundung den Befall von Krankheiten und Schädlingen (z.B. die Pilzkrankheit „Ojo de Gallo“) rechtzeitig großräumig auf Landschaftsebene zu erkennen und notwendige Maßnahmen überbetrieblich und eventuell staatlich zu ergreifen. Hierfür können zusätzlich Drohnen auf Grund ihrer relativ leichten Einsetzbarkeit und geringeren Wetterabhängigkeit zum Einsatz kommen.

5 Zusammenfassung und Fazit

Mit der Entwicklung der digitalen, auf DNS basierten Plattform für Agrardaten, wird die Sicherheit und das Vertrauen der Agrardaten erhöht. Das leichtgewichtige Identitäts- und Zugriffsmanagement im digitalen Ökosystem ermöglicht die Verifizierung der Sensor-Echtheit und stellt zusätzlich sicher, dass nur autorisierte Personen die Daten erhalten. Die Kombination aus dezentralen Zugriffskontrolllisten und zentraler Zugriffsrechtevergabe sowie die Verwendung der existierenden, globalen Infrastruktur des DNS ermöglichen ein hohes Maß an Flexibilität und eine gute Skalierbarkeit auf große und dynamische Systeme sowie einen weltweiten Einsatzbereich.

Literaturverzeichnis

[GO17] goDAN: Global Open Data, www.godan.info, Stand: 24.11.2017.

[ID17] Industrial Data Space, www.industrialdataspace.org, Stand: 24.11.2017.

[LI17] LIGHTest, www.lightest.eu, Stand: 24.11.2017.

[Mo83a] Mockapetris, P.V.: Domain Names: Concepts and facilities, RFC882, IETF 1983.

[Mo83b] Mockapetris, P.V.: Domain Names: Implementation specificat., RFC883, IETF 1983.

[SA17] Smart Agri-Food, www.smartagrifood.eu, Stand: 24.11.2017.

[SF17] Smart Farm Systems Inc., www.smartfarm.ag, Stand: 24.11.2017.