

## „Situations-Fingerabdruck“ - Verwaltungsstruktur- übergreifendes automatisiertes Berechtigungsmanagement für landwirtschaftliche Daten nach sachbezogenen Kriterien

Arndt Kritzner<sup>1</sup> und Jens Teichmann<sup>2</sup>

### 1 Ausgangssituation

Durch die in vielen Fällen hohe Zahl an Arbeitsgängen und Prozessbeteiligten in der landwirtschaftlichen Produktion und im Herstellungsprozess von Nahrungsmitteln entstehen Datenbestände, die in hohem Maße fragmentiert sind (Abb. 1). Für eine durchgehende digitale Prozessabbildung im Hinblick auf Produkteigenschaften, Bodenzustand und Prozessoptimierung ist eine Zusammenführung der Inhalte aus unterschiedlichen Datensammlungen erforderlich [KNT2016].

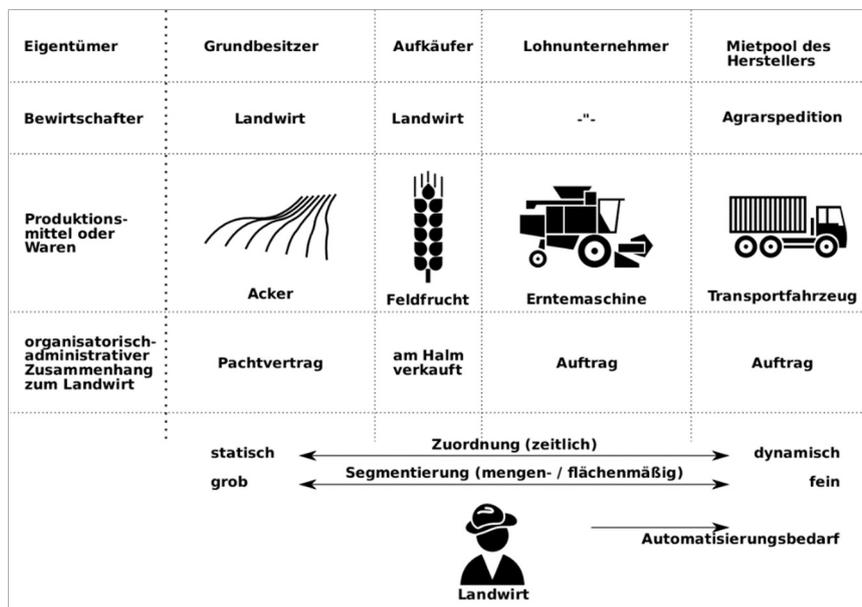


Abb. 4: Exemplarische organisatorische Struktur der landwirtschaftlichen Produktionsmittel und Waren für einen Ernteprozess

<sup>1</sup> Logic Way GmbH, Hagenower Straße 73, 19061 Schwerin, kritzner@logicway.de

<sup>2</sup> TU Dresden, Professur für Agrarsystemtechnik, 01069 Dresden, teichmann@ast.mw.tu-dresden.de

Die am Prozess beteiligten Produktionsmittel - Grund und Boden, Landmaschinen, Fahrzeuge, Verarbeitungsanlagen - sind im Besitz unterschiedlicher Parteien, so dass eine generelle Eigentümerschaft einer bestimmten Partei an allen Daten unmöglich sinnvoll bestimmt werden kann. Alle Prozessbeteiligten und letztendlich auch Verbraucher könnten von einem gegenseitigen Datenaustausch profitieren, der zu einer durchgängigen digitalen Abbildung der Abläufe und Zusammenhänge im landwirtschaftlichen Prozess führt.

## 2 Zielvorstellung

Aus sachlicher Motivation heraus ergeben sich verschiedene auszutauschende Dateninhalte (Abb. 2), deren Weitergabe an die jeweils betreffenden Prozessteilnehmer logisch und unstrittig erscheint. Dabei ist der Landwirt in aller Regel gleichermaßen Produzent und auch Konsument von Daten.

Bei Abfragen über Cloud-Betreibergrenzen hinweg muss gefordert werden, dass nicht bereits durch die Abfragen Information abfließt. Das wäre der Fall, wenn beispielsweise Uhrzeiten und Positionen von Gutübergabevorgängen im Klartext abgefragt würden.

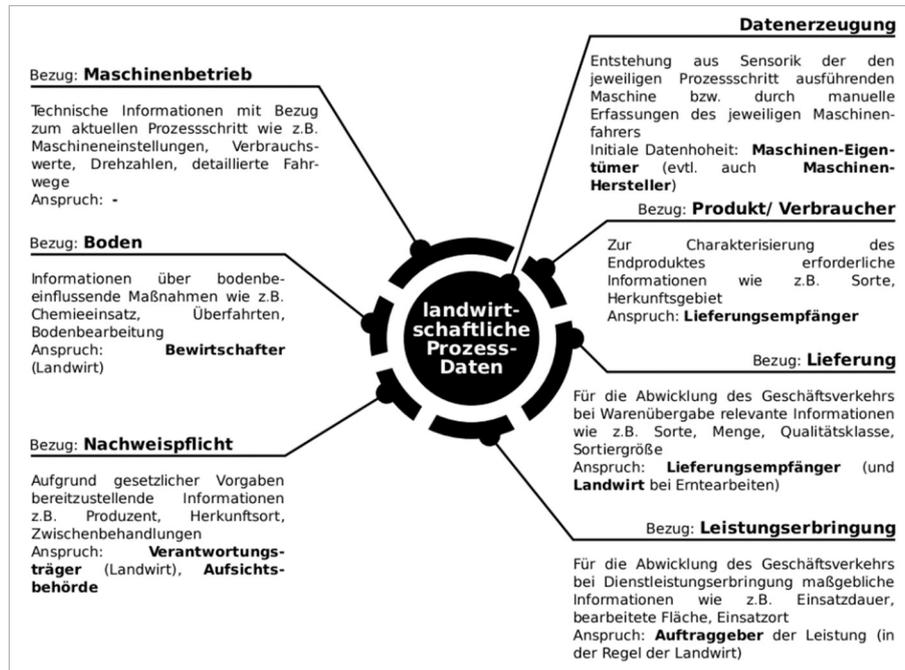


Abb. 5: Struktur für eine sachbezogene Datenverteilung

Die Identifikation der informationsaustauschenden Parteien und der auszutauschenden Datenportionen muss anhand von auf beiden Seiten vorhandenen Daten automatisiert erfolgen. Durch präzise Eingrenzung und Minimierung der zu übertragenden Dateninhalte wird Datensparsamkeit als Designkriterium umgesetzt und Datenschutz- und Geheimhaltungs-Belangen am ehesten Rechnung getragen.

### **3 Technisch-algorithmischer Ansatz**

Mit kryptografischen Verfahren ist es möglich, automatisiert einen kryptografischen Schlüssel zum qualifizierten Nachweis einer sachlichen Veranlassung zum Austausch einer bestimmten Datenportion zu errechnen. Die Abfrage des Schlüssels gegenüber den potentiellen Datenaustauschpartnern kann so gestaltet werden, dass für unberechtigte Empfänger der Abfrage keine Rückschlüsse auf den originalen Sachverhalt möglich sind. Für die Berechnung von Fingerabdrücken einer Interaktionssituation stehen typischerweise die Ausgangsgrößen Zeitpunkt, Ort, Menge und Sorte des ausgetauschten Gutes, Fahrgeschwindigkeit etc. zur Verfügung. Über nur vorwärts ausführbare Rechenoperationen können dabei beide an der realen Interaktion beteiligten Parteien zum gleichen berechneten Situations-Fingerabdruck gelangen.

Als Ausgangsparameter für die Berechnung des Situations-Fingerabdrucks muss sowohl auf der anfragenden als auch auf der angefragten Seite exakt dieselbe Folge derselben Werte codiert werden. Um von beiden Seiten reproduzierbare Werte physikalischer oder geografischer Messgrößen zu erhalten, ist die Verwendung eines Quantisierungsrasters erforderlich [BP2017].

Da mit jedem Fingerabdruck jeweils nur die Freigabe für einen kleinen Datenausschnitt einhergeht, sind keine allerhöchsten Sicherheitsanforderungen für den jeweiligen gebildeten Hash zu erfüllen.

Die am Informationsaustausch teilnehmenden Cloud-Datenbanken sind zweckmäßigerweise gleichberechtigt in Form einer Liste in einem Pool organisiert und erhalten alle dieselben Anfragen. Beantwortet wird eine Anfrage nur von dem Austauschpartner, der sich für den jeweilig angefragten Situations-Fingerabdruck qualifizieren kann.

Ausgehend von den eigenen bzw. den vorab ausgetauschten Verfahrensparametern wird über Quantisierung, Hash-Berechnung [BP2017] und Anfragemustergenerierung (Abb. 3) die Informationsaustausch-Anfrage automatisch synthetisiert, mit der anschließend die Datenpool-Teilnehmer automatisiert abgefragt werden. Die „interessierte“ Datenpool-Instanz beantwortet die Informationsaustausch-Anfrage positiv, alle anderen ablehnend ohne Informationsrückgabe. Nach Prüfung der vom Interessenten zurückgegebenen Antwortfolge auf die präsentierten Hashwerte wird die dadurch festgelegte Datenportion dem Anfrager bereitgestellt.

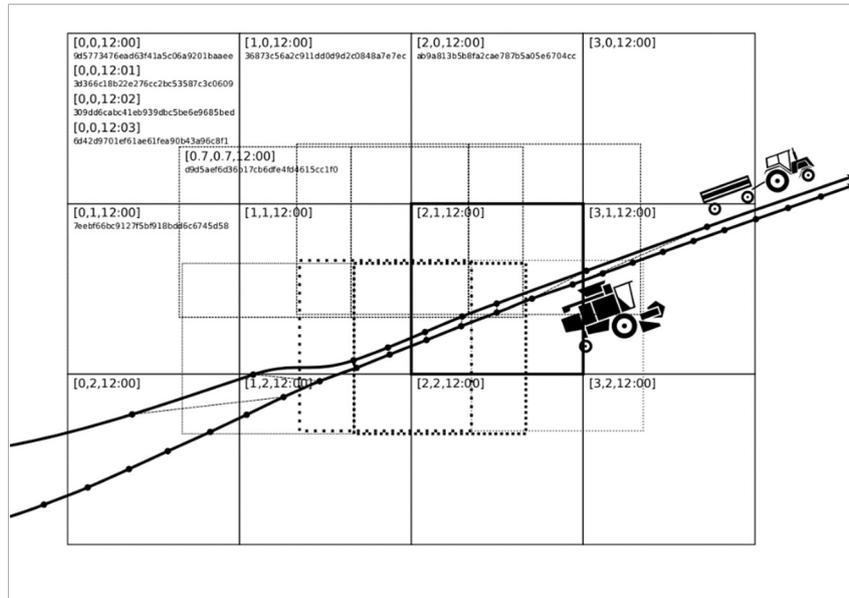


Abb. 6: Erzeugung eindeutiger und unumkehrbarer Identifikatoren für Ort-Zeit-Situationen – beispielhaft für eine Gutübergabe

#### 4 Organisatorische Umsetzung

Mit der Errechnung des Situations-Hash-Wertes zu einer Datenportion steht ein automatisiert berechenbares Merkmal für den Nachweis der Berechtigung einer Datenaustausch-Anforderung zur Verfügung. Dadurch kann automatisiert jeweils im Einzelfall auf sachlicher Basis über die Weitergabe von Daten entschieden werden. Potentiell zum Datenaustausch in Frage kommende Datenbanken können insgesamt als Pool abgefragt werden. Die Identifikation des angesprochenen Datenbestandes und der darin enthaltenen nachgefragten Datenportion wird durch den Hash-Wert geleistet. Letztendlich sind nur die gegenseitige Kenntnis der unterschiedlichen Cloud-Datenbestände und deren Teilnahme am Verfahren erforderlich.

##### Literaturverzeichnis

- [KNT16]: Kraatz, Franz; Nordemann, Frank; Tönjes, Ralf, Datensicherheit: Die nächste große Herausforderung in der modernen Landtechnik?, GIL Jahrestagung, 2016
- [BP17]: Böhme, Rainer; Pesch, Paulina, Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie, Datenschutz und Datensicherheit-DuD 41.8 (2017), 2017