# Chapter 2
# Related Work

The following chapter presents findings on selected related work and places my work in the corresponding context. There are two categories of related work with relevance to my work that are considered in this chapter:

- Related work dealing with access control, which is a special mechanism to expose data to authorized parties only, is presented in Sect. 2.1, and
- Related work dealing with EPCglobal networks and securing its components is presented in Sect. 2.2.

The first category is considered to outline existing techniques for protection of sensitive data, their limitations, and their applicability with respect to EPCglobal networks. The second is considered to present and evaluate standards introduced by the EPCglobal consortium, derive trends of ongoing security activities in this context, and to introduce the technical foundations of EPCglobal networks. In Sect. 2.3 the analysis results of related work are classified.

## 2.1 Access Control Mechanisms

Security aspects are typically researched to address a certain threat, platform, software, use case, etc. In the following, I place my work in context of related work on access control systems.

I define *access control* as all efforts to limit various actions $a \in A$ to sensitive resources $r \in R$ to a certain user $u \in U$. Access control can formally be defined as a triplet as given in Eq. 2.1. In context of EPCglobal networks, I focus on event data as the resources that need to be protected, i.e. $R = \{\text{EPC events}\}$.

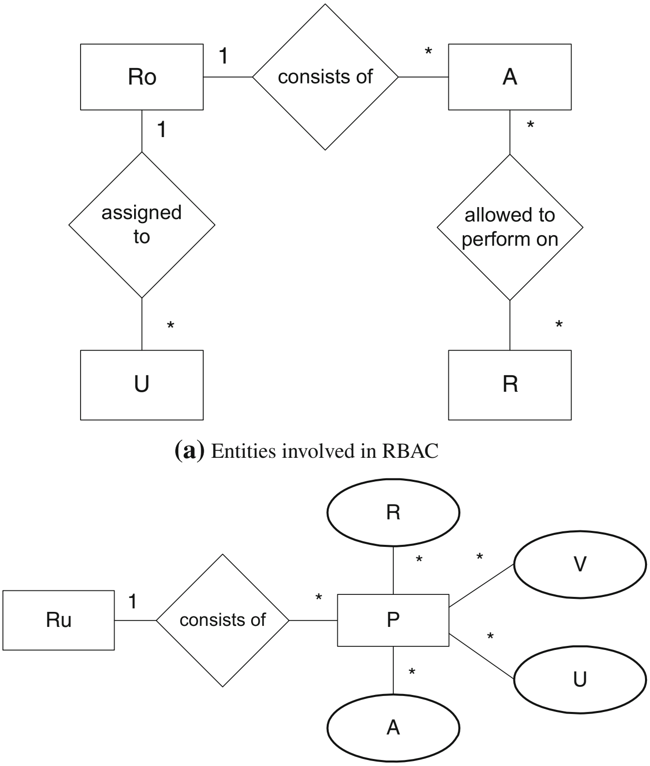
$$(a, r, u) \forall a \in A, r \in R, u \in U \tag{2.1}$$

Discretionary Access Control (DAC) describes a class of mechanisms that controls access by leaving the access decision to the user [1]. In other words, once a certain user is granted access to a resource, she/he is able to grant access for a certain

Matthieu-P. Schapranow, *Real-time Security Extensions for EPCglobal Networks*,
In-Memory Data Management Research, DOI: 10.1007/978-3-642-36343-6_2,

resource to further users. Even if there is only limited access defined for a certain resource, e.g. read-only, the user is able to create a copy of the resource's content and grant individual access for further users to the copied content, which results in data exposure. For example, representatives of DAC are Access Control Lists (ACLs) incorporated by the operating system Microsoft Windows and owner-group-other flags of Unix for controlling access to files. The counterpart of DAC is referred to as Non-Discretionary Access Control (NDAC), i.e. access is not directly controlled by the user, but by a dedicated administrative entity [1].

**Role-Based Access Control:** Role-based Access Control (RBAC) defines a superclass for access control mechanisms that enforce access rights and restrictions on working roles rather than on individuals [2]. RBAC decouples user management from access management. To do so, RBAC controls access to resources by controlling actions *A* performed by users *U* on resources *R*.



**(a)** Entities involved in RBAC

**(b)** Entities involved in RuBAC

**Fig. 2.1** Comparison of access control mechanisms using entity relationship diagrams: (**a**) RBAC controls allowed actions on resources via roles while (**b**) RuBAC controls access via rules evaluating predicates (*A* actions, *P* predicates, *R* resources, *Ro* roles, *Ru* rules, *U* users, *V* additional decision data)

In contrast to traditional access control, RBAC groups allowed actions $A$ in roles $Ro$ as depicted in Fig. 2.1a. There is no direct mapping between resources $R$ and users $U$ due to the indirection introduced by the roles concept. Formally, RBAC can be understood as set of tuples with $A_{ro} = (\{a \in A|$ permitted by $ro\}, R_{ro} = \{r \in R|ro$ is granted access to $\})$ and $U_{ro} = (\{u \in U|$ assigned to $ro\})$ as defined in Eq. 2.2.

$$RBAC = \{(A_{ro}, R_{ro}) \times U_{ro}\}, ro \in Ro \tag{2.2}$$

With the assumption that the number of users is larger than the number of active roles, RBAC results in reduced maintainability. For example, granting access to the location attribute of gathered event data to all colleagues working as packers becomes a single task. Rather than identifying all packers within the company and setting their individual access rights, all colleagues working as role `Packer` are assigned with the right to read EPC event location. Thus, all packers get immediate access to the required event data in a transparent way. Furthermore, also newly joined colleagues are automatically granted the access rights to read EPC event location. However, this results in the disadvantage, that people's role membership has to be supervised otherwise access rights might be expanded while certain persons are no longer allowed to get access. For instance, if there are two mutually excluding roles defined to establish a Separation of Duties (SoD) and a certain person is assigned to both roles, SoD is violated although RBAC is applied [1].

Nevertheless, I value RBAC as a concept that improves handling of access for a potentially infinite number of users. In terms of the pharmaceutical supply chain as described in Sect. 1.1 the number of users of a certain EPCIS repository is not known beforehand. In contrast to the number of involved goods and parties in the pharmaceutical supply chain, I expect the amount of active roles to be comparable small. Firstly, it is reasonable to distinguish between direct partners, who receive goods without involved third parties, and indirect partners, which receive goods via further intermediates roles in accordance with their place in the supply chain role. Secondly, roles can be used to group goods in categories and control access via this indirection. Thirdly, special classifications introduced by the supply chain party can be used to value certain partners, e.g. high and low priority business partners or suppliers.

This example shows two aspects of RBAC. Firstly, roles cannot be predefined due to the variety of possible classification criteria. Secondly, grouping individual inquirers into roles helps to abstract from the unknown number of inquirers and keeps access control as a limited task rather than as a regular task when an unknown inquirer is querying.

In context of EPCglobal networks and the given pharmaceutical scenario, RBAC supports abstraction of individuals. As a result, the administrative overhead for maintaining possibly hundred of thousands individual access rights vanishes. Thus, I consider RBAC as one way to reduce the complexity. In the given dissertation, RBAC is applied to definition and enforcement of access rights as described in Sect. 5.2.

**Rule-Based Access Control:** Rule-based Access Control (RuBAC) refers to all access control mechanisms defining access rights or restriction in a set of rules that need to be evaluated for each access request [1]. In other words, "RuBAC is a general term for access control systems that allows some form of organization-defined rules" [3]. RuBAC results in the advantage of defining various kinds of complex rules based on any kind of additional attributes, such as remote host name, current time, user details, etc. As a result, RuBAC enables a more fine-grained access control than RBAC. However, a concrete definition of rules and its interpretation needs to be implemented individually. RuBAC defines a set of rules *Ru* consisting of predicates *P* that are evaluated specifically when a concrete user *u* is accessing a certain resource *r* to perform an action *a*. Formally, RuBAC can be represented as given in Eq. 2.3 and depicted in Fig. 2.1b.

$$Ru = \{P(a, r, u, v)\}\}\forall a \in A, r \in R, u \in U, \{v \in V | \text{ decision data}\} \tag{2.3}$$

RuBAC results in a higher flexibility when granting access. In the given dissertation, RuBAC is incorporated to adapt access rights accordingly to the history of granted access rights as described in Sect. 5.2.

The contributed HBAC combines RBAC and RuBAC to control access to event data in a holistic way as described in Sect. 5.1.

**Extensible Access Control Markup Language:** The eXtensible Access Control Markup Language (XACML) is an eXtensible Markup Language (XML) dialect specified by the OASIS consortium. It aims to define access control rights for subjects representing users, resources, and action based on rules and policies [4]. In addition, XACML introduces a conceptual SoD for access control systems, which is also applicable for the given work. Table 2.1 presents XACML duties, its brief description and a mapping to components of my work with direct references for further reading.

The use of XML for definition of access rights is a common approach as shown by the classification of related work. This standardized way of communication contributes to the interoperability between various software systems and vendors. In addition, it makes the automatic transformation of data formats possible, e.g. by using an eXtensible Stylesheet Language Transformations (XSLTs) [5]. However, in addition to XACML, which is only rarely used for RFID-specific developments, various extensions or other XML dialects are used, such as aidXACML or EAL introduced by Grummt et al. [6].

**Open Digital Rights Language:** The Open Digital Rights Language (ORDL) is a XML dialect for defining and maintaining rights of asset [7]. Assets in context of ODRL are mainly multimedia contents, such as audio or video contents. In the given work, I consider event data as company-specific assets comparable to purchased multimedia contents. Event data can be accessed by various inquirers but with individual access rights. Once a certain criterion has expired accessing event data must no longer be possible. I decided to make use of ODRL for definition of access rights and access control information for my contribution since it is a

Table 2.1 Mapping of XACML duties to sections within this document

| XACML | Description | HBAC | Section |
|---|---|---|---|
| Policy Enforcement Point (PEP) | Component that enforces the decision issued by the PDP, i.e. interacting with the user and the resource to grant access to | Access Control Client (ACC) | 5.1.3 |
| Policy Decision Point (PDP) | Component that issues and revokes valid policies, e.g. based on external information, such as the querying user, history, context, etc. | Access Control Server (ACS) | 5.1.4 |
| Policy Administration Point (PAP) | Component responsible for managing policies, i.e. creating or modifying or access rights | Configuration Tool | 5.1.5 |
| Policy Information Point (PIP) | Component that provides additional information for the PDP to derive decisions | Trust Relationship Server (TRS) | 5.1.6 |

lightweight approach and reduces data processing overhead. However, a homomorphism can be defined that transforms ODRL to the more expressive XACML, i.e. XACML is another possible implementation for definition of access rights.

## 2.2 Components of EPCglobal Networks

The EPCglobal consortium—newly also known as Global Standards 1 (GS1)—defines technical components and standards for intercommunication in RFID-aided supply chains. EPCglobal standards can be grouped in the functional layers identification, capturing, and exchanging as depicted in Fig. 2.2 [8].

The *identification* layer deals with the data format stored on tags, e.g. Tag Data Standard (TDS), and its translation, e.g. Tag Data Translation (TDT).

The *capturing* layer defines the communication protocol between tags and readers, e.g. Tag Protocol UHF Class 1 Gen1, EPC HF, and the Low Level Reader Protocol (LLRP), which is responsible for data acquisition and event capturing. On top, the Discovery Configuration and Initialization (DCI) and the Reader Management (RM) define how to discover and control distributed reader devices. The Application Level Events (ALE) standard defines how to handle, filter, and process reader events for software applications.

EPCIS bridge the gap between the layers *capture* and *exchange*. The Core Business Vocabulary (CBV) defines language elements used for data exchange. From the enterprise's point of view, the EPCIS provides high-level access methods for processing event data in enterprise applications, such as ERP systems. Object Name Service (ONS) and EPCDS perform lookup and discovery of resources, such as supply chain participants that handled a certain good. The standards

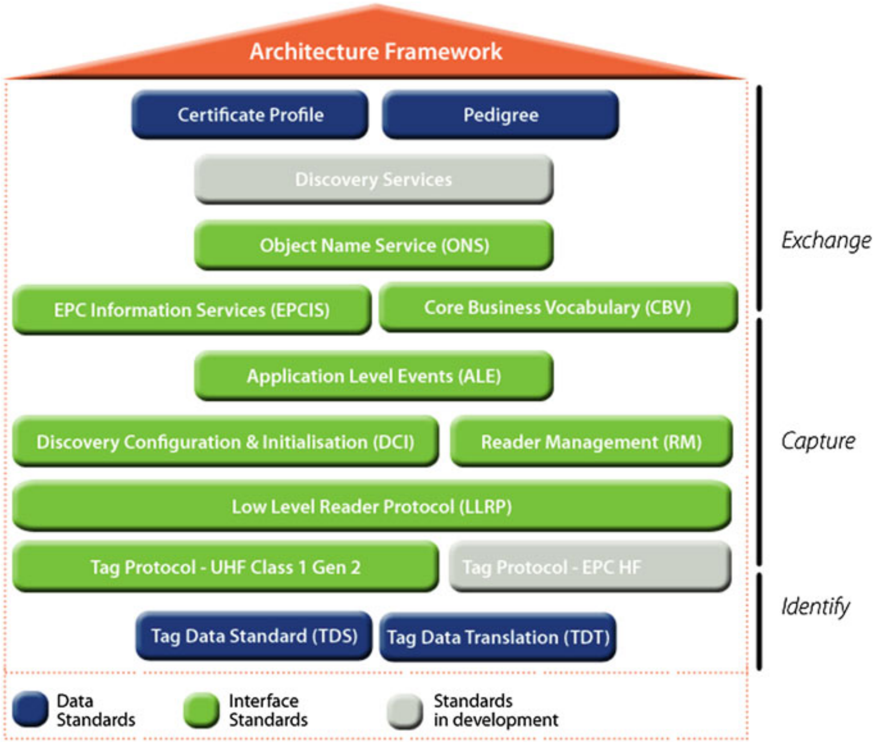

Architecture Framework
Certificate Profile
Pedigree
Discovery Services
Object Name Service (ONS)
EPC Information Services (EPCIS)
Core Business Vocabulary (CBV)
Application Level Events (ALE)
Discovery Configuration & Initialisation (DCI)
Reader Management (RM)
Low Level Reader Protocol (LLRP)
Tag Protocol - UHF Class 1 Gen 2
Tag Protocol - EPC HF
Tag Data Standard (TDS)
Tag Data Translation (TDT)
Exchange
Capture
Identify
Data Standards
Interface Standards
Standards in development

**Fig. 2.2** Stack of EPCglobal standards taken from [8]. It consists of the layers tag identification, capture, and exchange of event data with business applications

Certificate Profile (CP) and Pedigree define data formats for exchanging data within EPCglobal networks from a business perspective.

I define EPCglobal networks as communication networks that exchange event data with the help of the components as defined by EPCglobal standards of the appropriate layer. In other words, EPCglobal networks contain only relevant components for business transactions, i.e. EPCglobal actors for EPCIS, ONS, and EPCDS. In addition to existing EPCglobal definition, I assume the existence of a generic service provider that performs business tasks not addressed by aforementioned components of EPCglobal networks, such as anti-counterfeiting.

*RFID Tags*

RFID tags consist of the components: (a) antenna, (b) integrated circuits, (c) data storage, and (d) optional equipment, such as sensors. They are tiny radio devices that can be distinguished according to (a) the operating frequency band, (b) the type of tag, and (c) their read-write capabilities.

**Frequency Bands:** The available radio band for RFID communication is defined by global standardization that can be restricted on a per-country basis [9].

**Table 2.2** Classification of radio frequency bands used by RFID tags

| Radio band | Frequency |
|---|---|
| Low Frequency (LF) | 100–135 kHz |
| High Frequency (HF) | 13.56 MHz |
| Ultra High Frequency (UHF) | 868 MHz (Europe), 915 MHz (USA), 2.45 GHz (ISM) |
| Super High Frequency (SHF), Micro Wave (MW) | 5.8 GHz |

UHF tags are nowadays used for tracking and tracing scenarios due to the low power required for emitting signals

Table 2.2 gives an overview of available radio bands and their frequency in Europe and in the United States of America (USA). In comparison, current radio broadcasting based on FM operates in the frequency band 87.5–108 MHz, whereas former radio broadcasting was based on AM that operates in the frequency band Long Wave (LW) 148.5–283.5 kHz, Medium Wave (MW) 520–1,610 kHz, and Short Wave (SW) 2.3–26.1 MHz [10]. Furthermore, current cellular phones operate in the bands 900–1800 MHz (Europe), 850–1900 MHz (USA) respectively [11, Sect. 2.1]. Nowadays, UHF tags are mainly used for EPCglobal networks, i.e. their operating frequency is comparable to cellular phones or is located within the so-called Industrial, Scientific, and Medical (ISM) band.

**Tag Types:** The tag’s type describes its capabilities. Keeping production costs low is a major requirement for passive RFID tags in EPCglobal networks for Near Field Communication (NFC) [12, Chap. 3]. Passive low-cost tags are powered by the physical principle of induction, i.e. they need to be placed near the reader’s electromagnetic field, which is required for (a) power supply of the tag’s integrated circuits and (b) data communication. In contrast to NFC, Far Field Communication (FFC) refers to communication when the distance between reader and tag exceeds one wavelength [13, Sect. 4.2.1.1]. FFC requires typically active RFID tags since they are able to actively modulate data via the radio band using their equipped battery. Table 2.3 compares the classification of tag capabilities.

**Table 2.3** Classification of RFID tag types

| Type | Functionality | Description |
|---|---|---|
| Passive | Induction | No power supply, powered by reader’s electromagnetic induction, works only while in the reader’s field |
| Semi-active | Induction, $\mu C$ | Battery-powered, e.g. to perform regular sensor measurements, not for transmission |
| Active | Active transmission, $\mu C$ | Battery-powered to extend transmission range and for regular sensor readings |

Passive tags work only with an external stimulus. They are used due to their low manufacturing costs for nowadays tracking and tracing scenarios

**Table 2.4** Read-write capabilities of RFID tags

| Type | Description | Example |
|---|---|---|
| Read-only | Programmed once by the tag's manufacturer, | Toll systems, e.g. E-ZPass [14] |
| Write-once, Read-many | Programmed once by the product's manufacturer | Tags with EPCs [12] |
| Read-write | Content can be changed at any time | Cash card systems, e.g. PUCK [15] |

Read-only tags are nowadays used for tracking and tracing scenarios due to the higher hardware requirements for read-write tags

**Read-Write Capabilities:** Read-write capabilities of RFID tags can be used to further classify tags. Three classes of tags exist according to their read-write capabilities: (a) read-only, (b) write-once, read-many, and (c) write-many, read-many tags [12, Chap. 7]. Table 2.4 gives a comparison of RFID tags based on its read-write capabilities. Read-only tags are a subset of Write-Once Read-Many (WORM) tags, but the tag's manufacturer initializes its content. The first user, e.g. the goods' manufacturer, initializes write-once, read-many tags. Write-many, read-many tags are equipped with a small flash storage comparable to external flash devices for personal computers that can be read and written multiple thousand times.

*RFID Reader*

RFID reader devices consist of (a) a set of antennas and (b) a controller device. The controller device implements radio interface protocols to communicate with RFID tags via the ether. Antennas are used to send out radio signals to tags and to receipt data.

*Object Name Service*

The ONS is a yellow page service for RFID-aided supply chains [16]. It returns for a given EPC the Unified Resource Locator (URL) of the manufacturer's EPCIS. The inquirer can contact the EPCIS of the manufacturer to obtain further details about the product and subsequent participants that handled a certain good identified by the EPC.

*EPC Information Services*

The EPCIS provides standardized interfaces between internal event repositories and external inquirers [17]. In other words, it is responsible for exchanging relevant internal data with external participants of the supply chain, e.g. to perform anti-counterfeiting. The EPCIS is also involved in controlling access to event data and to ensure privacy of internal data. Thus, I consider the EPCIS as a possible target of attackers to obtain event data.

*EPC Discovery Services*

The EPCDS acts as an intermediate for querying parties that pre-processes data from various EPCIS repositories and performs preliminary operations on them, e.g. aggregation of internal event data [18]. When the inference concept for supply chains is applied, the EPCDS is required to reconstruct the virtual path of individual products. Up to now, there is no EPCDS implementation ratified by EPCglobal available since corresponding standards are still in development. However, Müller contributes with an EPCDS built on the in-memory building blocks as defined in Sect. 3.4 [19].

*Middleware*

The RFID middleware acts as a mediator between RFID readers and the capturing interface of the EPCIS repository. It fulfills a set of common tasks within a company to integrate event data in existing business systems, such as ERP systems. Furthermore, it is responsible for filtering and collecting events and for the harmonization of data format between EPCglobal components [17].

*Security in EPCglobal Networks*

The Certificate Profile (CP) is defined by the EPCglobal consortium and specifies security aspects in EPCglobal networks. The first version 1.0 was released in March 2006 and contains the sections "Introduction", "Algorithm Profile", "Certificate Profile", "Certificate Validation Profile", and two appendices, which are described in a total of 11 pages [20]. Latest released version 2.0 ratified in June 2010 consists of the identical outline in a total of 14 pages [21]. In the following, the content of the latest CP is summarized and evaluated.

The CP expects the use of X.509 certificates in context of EPCglobal networks, which requires a global PKI. From my perspective, this is feasible, since the use of PKIs has been proven to work for productive environments, such as device and user authentication 802.11x in communication networks and Germany's electronic identity cards [22, 23]. The rest of the CP provides recommendations about the use of X.509 certificates for identification purposes.

The section "Algorithm Profile" contains recommendations for X.509 certificates. As of today, it is recommended to use the following settings:

- Algorithm: sha2WithRSAEncryption, i.e. any of the algorithms SHA-224, SHA-256, SHA-384, SHA-512.
- Key length: 2,048 bits (3,072 bits by the year 2031).

The section "Certificate Profile" contains mainly a description on how to include an EPC's URI representation within a certificate and how to encode users, services, servers, readers and devices accordingly, e.g. by including their unique serial number and/or device specific Media Access Control (MAC) identifier [24].

Further details about how to ensure security aspects, such as authentication and how to use it in context of access control are not defined in the CP. Therefore, I evaluated the latest EPCIS standard version 1.0.1 ratified in September 2007 for definitions regarding security [17]. It contains a subsection dealing with authentication and one dealing with authorization. The former contains the indication that the EPCIS Query Control Interface can be used for authentication. In addition, a "non-normative explanation" is given, indicating that the use of mutual authentication is expected. Concrete implementations or definitions are missing. The section about authorization specifies the following actions as valid:

- Refuse a request completely by a generic `SecurityException`,
- Hide data, e.g. the list of business transactions, but remove entire event when hiding data results in misleading data,
- Return a subset of requested data only, e.g. only the first hundred matching events when querying all known events,
- Respond with coarser grained data than requested, e.g. substituting all company-internal locations, such as gate 1, assembly area 2, etc. by a common location for the company, and
- Limit the scope of a query to a certain client, e.g. to provide EPCIS repositories as Software-as-a-Service (SaaS) [25].

The business-level security extensions described in Chap. 5 incorporate the latter three aspects to restrict access of clients to event data. The CP contains further a "non-normative explanation" stating: "[...] the EPCIS specification does not take a position as to how authorization decisions are taken" [17]. I value my work as a concrete contribution to show how to handle these decisions and how to protect sensitive event data.

The term *security services* was recently mentioned in the context of EPCglobal standards. However, an actual definition or a draft is still missing during creation of this document. I consider the results of this work as a major step towards making security services for EPCglobal networks come true.

Official standards provide clues for incorporating security features and expect their usage. However, EPCglobal leaves detailed design decisions, implementation strategies, and concrete implementations are left open to the reader. These standards lack a comprehensive description of threats, attack scenarios, their impact on business processes and possible countermeasures. The transformation of a conventional supply chain towards an RFID-aided supply chain involves various security relevant adaptations, such as open interfaces for accessing EPCIS repositories [17]. Existing work shows various threats, their impact, and countermeasures. The given dissertation contributes in designing, developing, and implementing concrete security extensions for EPCglobal EPCIS repositories. The latter is considered as a possible target of attacks since it is the source of sensitive event data that can be misused by attackers to derive correlated business information [26].

## 2.3 Combination and Classification of Related Work

**Historic Developments:** The wish for data protection in information systems is as old as the existence of any kind of data. Historically speaking, during the early development of first computer systems in World War II, such as ENIAC, the aspect of data protection arose [27]. For instance, with the invention of radar systems airplane attacks could be detected by sending out a radio signal and observing its reflections [14]. Identification Friend or Foe (IFF) systems were developed to distinguish unknown aircrafts from each other. Friendly aircrafts were equipped with an IFF system that sent out a special signal in response to a detected radar signal [28]. Let us consider IFF systems as information systems since typical attacks for information system also apply for them. Further details about concrete threats for RFID-aided supply chains are described in Sect. 3.1. After introducing IFF systems, they were copied and security extensions, such as on-device encryption, were added to secure their operation [28].

Lampson defines "[...] all the mechanisms that control the access of a program to other things in the system" [29] as *protection*. This general definition contains the first indication of the nowadays more popular term *access control*. In his work, the primarily goal of adding protection to information systems is named as protecting users from their own or other users' malice. In context of my work, this is still valid, since the goal is to protect supply chain participants from malicious behavior—whether intended or unintended—of other supply chain participants, technical errors of other automatic information systems, competitors, counterfeiters, or any kind of attackers. In addition, Lampson discusses concepts of *access control matrices* as a strategy for protection. This concept is also incorporated by the given work. He names possible issues that reside in former hardware limitations of the year 1971. For instance, the complete access control matrix can grow fast depending on the amount of users and objects. Keeping it entirely in fast accessible main memory, is considered as a waste of resources since its capacity is limited and only single entries of the access control matrix need to be accessed at a certain moment [29].

In my work, I consider these hardware limitations as no longer valid. I keep the entire access control matrix in a compressed format in fast access main memory by incorporating in-memory technology as discussed in Sect. 3.4.

The historical examples show a common empiric paradigm that is still valid for modern information systems: aspects of data protection are rarely considered during the design phase. More often, data protection is investigated once a product is ready to sell and a critical number of users are running the system. After this critical mass has been reached, the product becomes a more attractive target for attackers. In context of EPCglobal networks, the EC has recognized this gap for RFID systems and released a recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification in 2009. It contains the explicit advice to overcome the gap of security by recommending that "[...] privacy and information security features should be built into RFID applications before their widespread use (principle of 'security and privacy-by-design')" [30]. In addition, it contains a list of guidelines and principles that should be considered while implementing RFID information systems to raise its acceptance.

**Risk Assessment:** From the risk assessment's point of view, classifications of security risks are helpful to identify threats, assess them, evaluate their monetary impact, and to design and implement countermeasures [31]. Garfinkel et al.

classify security risks accordingly to the location where they occur in one of the following classes [32]:

- **Inside the Supply Chain**: Locations and transportation systems controlled by supply chain participants,
- **Outside the Supply Chain**: Locations after the product left the control of supply chain partners and is operated by the customer, and
- **In the Transition Zone**: Locations when products are leaving from inside to outside the supply chain, e.g. when the product is handed to the customer.

The given work primarily addresses the security of event repositories and the involved data exchange. Thus, I address threats that belong to the categories inside the supply chain and within the transition zone.

Spiekermann performed neutral studies on the acceptance of RFID technology and Privacy Enhancing Technologies (PETs) in retail businesses. In her work, she comes to the result that "[...] consumers do value the service spectrum, which can be realized through RFID [but] they are willing to forgo these benefits in order to protect their privacy" [33]. As a result, I stress the fact that improving security by using transparent privacy protection mechanisms is mandatory to increase acceptance for RFID-aided supply chains.

In 2006, the National Institute of Standards and Technology (NIST) published a technical report assessing access control systems. It observes that a wide range of access control systems is based on XML-based policy languages, but all of them lack the capability to express historical-based policies [1, Sect. 3.6.3]. In context of EPCglobal networks the temporal and history aspect becomes more important since goods are moving from party to party and access rights need to be modified multiple times during the lifecycle of a certain product. During my research of related work for EPCglobal networks, I observed only a small amount of related works dealing with temporal access control [1, 34]. This has motivated me to focus on processing of the query history to contribute with an HBAC system based on in-memory data processing in the given work.

**Classification:** In the following, I classify related work corresponding to their categories: (a) related work dealing with access control management systems and (b) RFID-specific related work. Figure 2.3 depicts components of an RFID information system that might be addressed by RFID-specific work. Table 2.5 categorizes these components correspondingly to their physical location within the supply chain and their technology affinity. It shows that RFID tags and readers are systems embedded in hardware to perform frequent actions in a very fast response time. In contrast, the remaining components are software system components of the enterprise software architecture. As a result, different requirements for interoperability and standardization exist for both categories. The classification in internal and external components is the basis to identify security threats. Company internal components can be controlled by enterprise-wide security policies that are enforced by regular trainings or tests of personnel. In contrast, external components cannot be controlled by company policies. Therefore, external components

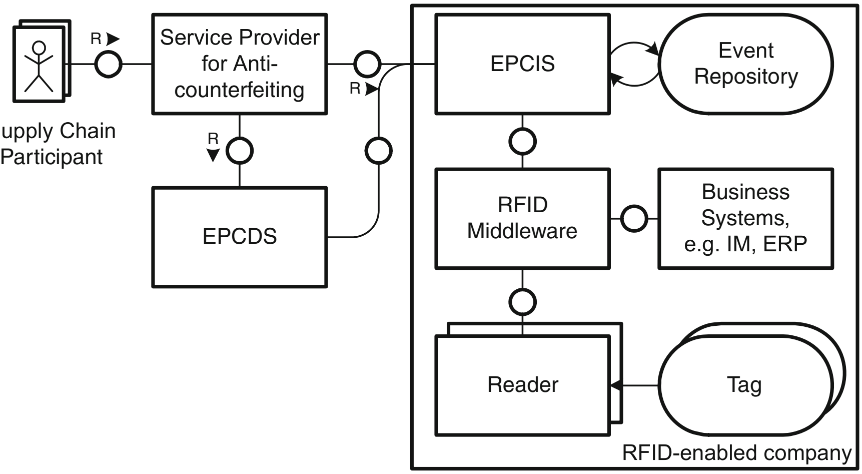


**Fig. 2.3** Infrastructure components of RFID-enabled companies depicted as FMC block diagram. Company-internal and -external systems exchange event data through standardized interfaces of EPCIS as defined by EPCglobal

**Table 2.5** Classification of components of RFID information systems

| Component | Location | Category | Type |
|---|---|---|---|
| EPCIS repository | Company/SaaS provider | E/I | SW |
| RFID middleware | Company | I | SW |
| RFID reader | Company, freight gates, stock, etc. | I | HW |
| RFID tag | Good | E | HW |
| Service provider | SaaS provider | E | SW |
| Discovery service | SaaS provider | E | SW |

*E* external, *HW* hardware, *I* internal, *SW* software. Two-thirds are software components

should be considered as uncontrollable components in terms of security that might be the foundation of further threats [35]. Two thirds of the components given in Table 2.5 are software, whereas I categorized the EPCIS repository as internal and external component equally. In this work, I focus on how to secure internal and external components, i.e. passive RFID tags and EPCIS repositories. The need for focusing on software components arises from the evaluation of components and categories addressed by related work.

Figure 2.4 visualizes the results of my analysis of related work. It depicts the year of publication in relation to the addressed RFID component and quantity of publications. Starting in 2005, it shows that related work dealing with security focuses on the air interface between readers and tags. Due to the limited security capabilities of low-cost tags and uncontrollable vulnerable environments the tag's content can be obtained with various well-researched techniques. For further details please refer to Chap. 4. Moreover, Fig. 2.4 highlights two further

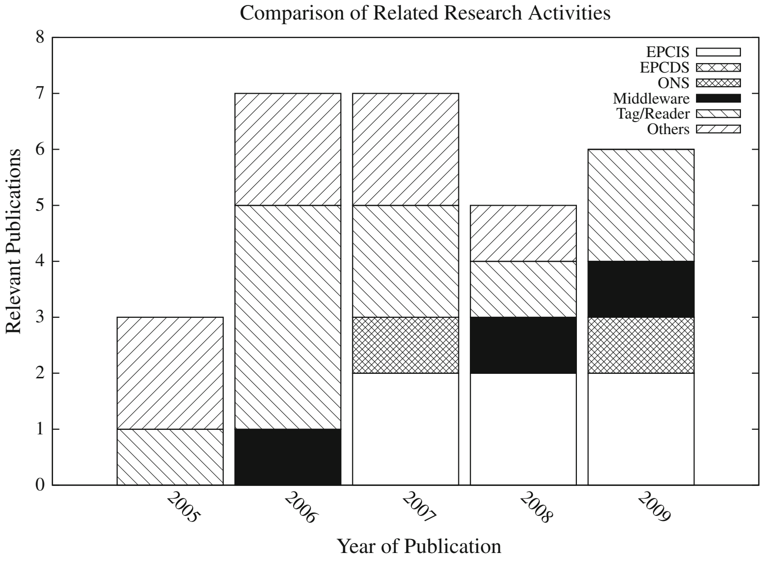


**Fig. 2.4** Comparison of related work depicting year of publication (2005–2009) versus addressed component and amount of relevant publications. Until 2007, Publications addressing security of components tags, readers, and their communication dominate. From 2008 on, Work addressing security of software systems, such as EPCIS repositories, middleware, and ONS, dominate. Work addressing the security of EPCDS is not present

characteristics of related work: (a) research activities concerning security of enterprise components started after device-level security was researched and (b) work dealing with security aspects of enterprise components of EPCglobal networks rarely exist in comparison of work addressing the air interface, tags, or reader hardware. Although switching to EPCglobal networks involves new hardware components, e.g. RFID readers for RFID technology or barcode scanner when incorporating visual identification techniques, various software components are also required. Table 2.5 classifies components of RFID-aided supply chains according to the category's location within the supply chain, its access type, and whether it is a hard- or software component. It highlights that the amount of involved enterprise software components, such as EPCIS repository, EPCDS, ONS, etc., is twice the amount of involved hardware components. The majority of involved enterprise software components motivate my research activities on business-level security in the rest of my work.

A similar trend can also be observed for industrial implementation projects, e.g. for product authenticity. For example, the pharmaceutical manufacturer Pfizer started a pilot project to use RFID technology for tracking pharmaceuticals in 2006, but it was not rolled out company-wide, until today [36]. The Metro Future Store initiative aims to improve supply chain management in the last step of supply chain: in retail stores, but most of the examples lack concrete productive implementation [37]. Public discussions about the reasons for stopping these projects are not available. However, concerns about data security and privacy are considered as possible reasons [33]. Initiatives, such as FoeBuD e.V. in Germany, fight for a strict use of RFID tags in industries, e.g. in retail stores [38]. Figure 2.4 depicts that these privacy concerns are addressed by related work for securing RFID-specific enterprise systems starting in 2007. This dissertation contributes by providing security extensions for RFID-specific enterprise software components to increase the acceptance and the future usage of EPCglobal networks.

My dissertation combines access control mechanisms, EPCglobal networks, and RFID technology as individual fields of research. I have analyzed existing related work with respect to each of the research fields focusing on data security and applicability to the given pharmaceutical scenario in Sect. 1.1. Table A.2 in Appendix A.1 classifies related work in the area of access control mechanisms corresponding to their technique specifics and their type of contribution. For example, Abadi and Fournet discuss the dynamic assignment of access rights for programs during their execution and refer to it as HBAC [39]. Edjlali et al. proposed years ago that HBAC "[...] has the potential to significantly expand the set of programs that can be executed without compromising security [...]" [40]. The NIST observed that concrete HBAC implementations are limited, e.g. in terms of real-time analysis of the history [1].

Based on the given components, related work dealing with RFID-specific data security and privacy threats is classified in Tables A.3–A.7. The comparison shows with respect to latest access control approaches a common usage of XML-based approaches for specification of access rights; primarily XACML, which is discussed in the following. Furthermore, there is a two-divided implementation approach for data security in RFID technology. For securing the communication between tag and reader fast hardware-based implementations are incorporated. However, the majority of related work dealing with EPCglobal components proposes software solutions, e.g. when focusing on the aspects authentication or access control. Only a small portion of related work actively makes use of encryption when exchanging data. I assume that most contributions do not consider data security in EPCglobal networks so far due to the missing standardization of the EPCglobal consortium.

## References

1. V.C. Hu, D.F. Ferraiolo, D.R. Kuhn, Assessment of Access Control Systems. Interagency Report 7316, National Institute of Standards and Technology (2006)
2. D.F. Ferraiolo, D.R. Kuhn, Role-based access control, in *Proceedings of the 15th NIST National Computer Security Conference* (1992), pp. 554–563
3. A.S. Sodiya, A.S. Onashoga, Components-based access control architecture. Issues Inf. Sci. Inf. Technol. **6**, 699–706 (2009)
4. OASIS Open. eXtensible Access Control Markup Language (XACML) V.2.0, Feb 2005
5. J. Clark, XSL Transformations (XSLT) (1999), http://www.w3.org/TR/xslt. Accessed 8 Mar 2012

6. E. Grummt, M. Schöffel, Verteilte Autorisation in RFID-Ereignissystemen, in *D.A.CH Security: Bestandsaufnahme, Konzepte, Anwendungen, Perspektiven*, ed. by P. Horster (Berlin, 2008) pp. 337–345
7. ODRL Initiative: ODRL V2.0 - XML encoding (2010), http://odrl.net/2.0/WD-ODRL-XML.html. Accessed 8 Mar 2012
8. Global Standards 1: GS1 standards knowledge centre (2011), http://www.gs1.org/gsmp/kc/epcglobal/. Accessed 8 Mar 2012
9. International Organization for Standardization, ISO/IEC 18000: Information Technology—Radio Frequency Identification for Item Management, 2004–2010
10. International Telecommunication Union, ST61 Agreement (2011), http://www.itu.int/ITU-R/terrestrial/broadcast/plans/st61/index.html. Accessed 8 Mar 2012
11. A. Selian, 3G mobile licensing policy: from GSM to IMT-2000—a comparative analysis technical report, International Telecommunication Union (2001)
12. E.C. Jones, C.A. Chung, *RFID in Logistics: A Practical Introduction* (CRC Press, Boca Raton, 2007)
13. K. Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication*, 2nd edn. (Wiley, New York, 2010)
14. M. Roberti, The history of RFID technology. RFID J. 1–3 (2008)
15. Heydt-Benjamin et al., Vulnerabilities in first-generation RFID-enabled credit cards, in *Financial Cryptography and Data Security*, volume 4886 of Lecture Notes in Computer Science, ed. by S. Dietrich, R. Dhamija (Springer, Berlin, 2007), pp. 2–14
16. Global standards 1: EPCglobal object name service 1.0.1 (2008), http://www.gs1.org/gsmp/kc/epcglobal/ons/ons_1_0_1-standard-20080529.pdf. Accessed 8 Mar 2012
17. Global Standards 1: EPCIS standard 1.0.1 (2007), http://www.gs1.org/gsmp/kc/epcglobal/epcis/epcis_1_0_1-standard-20070921.pdf. Accessed 8 Mar 2012
18. Global Standards 1: discovery services standard (in development) (2011), http://www.gs1.org/gsmp/kc/epcglobal/discovery. Accessed 8 Mar 2012
19. J. Müller, An in-memory discovery service to retrieve track & trace information in a unique identifier network with hierarchical packaging (to appear), Ph.D. thesis, Hasso Plattner Institute, 2012
20. Global Standards 1: EPCglobal certificate profile specification version 1.0 (2010), http://www.gs1.org/gsmp/kc/epcglobal/cert/cert_1_0-standard-20060308.pdf. Accessed 8 Mar 2012
21. Global standards 1: EPCglobal certificate profile specification version 2.0 (2010), http://www.gs1.org/gsmp/kc/epcglobal/cert/cert_2_0-standard-20100610.pdf. Accessed 8 Mar 2012
22. The Institute of Electrical and Electronics Engineers, Inc, Wireless LAN medium access control (MAC) and physical layer (PHY) specifications (2010), http://standards.ieee.org/getieee802/download/802.11z-2010.pdf. Accessed 8 Mar 2012
23. Bundesamt für Sicherheit in der Informationstechnik: BSI TR-03128 EAC-PKI'n für den elektronischen Personalausweis, V. 1.1 (2010), https://www.bsi.bund.de/ContentBSI/Publikationen/TechnischeRichtlinien/tr03128/index_htm.html. Accessed 8 Mar 2012
24. The Institute of Electrical and Electronics Engineers, Inc., EEE standard for local and metropolitan area networks: overview and architecture (2002), http://standards.ieee.org/getieee802/download/802-2001.pdf. Accessed 8 Mar 2012
25. A. Benlian, T. Hess, P. Buxmann, *Software-as-a-Service: Kunden-Anbieterstrategien* (Kundenbedürfnisse und Wertschöpfungsstrukturen, Gabler, 2010)
26. M.-P. Schapranow, M. Lorenz, A. Zeier, H. Plattner, License-based access control in EPCglobal networks, in *Proceedings of 7th European Workshop on Smart Objects: Systems, Technologies and Applications*, VDE, 2011
27. M.-P. Schapranow, ENIAC tutorial: the modulo function (2006), http://www.myhpi.de/∼schapran/eniac/modulo. Accessed 8 Mar 2012
28. M.R. Rieback, B. Crispo, A.S. Tanenbaum, The evolution of RFID security. IEEE Pervasive Comput. **5**, 62–69 (2006)

29. B.W. Lampson, Protection, in *Proceedings of 5th Princeton Conference on Information Sciences and Systems* (1971), pp. 437–443
30. European Commission, Recommendation on privacy and data protection in applications supported by radio-frequency identification (2009), http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf. Accessed 8 Mar 2012
31. Federal Office for Information Security, BSI standard 100–3: risk analysis based on IT-Grundschutz V.2.5 (2008)
32. S.L. Garfinkel, A. Juels, R. Pappu, RFID privacy: an overview of problems and proposed solutions. IEEE Secur. Priv. **3**, 34–43 (2005)
33. S. Spiekermann, Privacy enhancing technologies for RFID in retail: an empirical investigation, in *Proceedings of the 9th International Conference on Ubiquitous Computing* (Springer, Berlin, 2007), pp. 56–72
34. E. Bertino, P.A. Bonatti, E. Ferrari, TRBAC: a temporal role-based access control model. ACM Trans. Inf. Syst. Secur. **4**, 191–233 (2001)
35. M.-P. Schapranow, J. Müller, A. Zeier, H. Plattner, Security aspects in vulnerable RFID-aided supply chains, in *Proceedings of 5th European Workshop on RFID Systems and Technologies*, VDE, 2009
36. US Pharmaceuticals Pfizer Inc., Anti-counterfeit drug initiative workshop and vendor display (2006),http://www.fda.gov/OHRMS/DOCKETS/dockets/05n0510/05N-0510-EC21-Attach-1.pdf. Accessed 8 Mar 2012
37. METRO Group, METRO group and RFID (2008), http://www.future-store.org/fsi-internet/get/documents/FSI/multimedia/pdfs/broschueren/RFID%20und%20MG-E-271108-Internet.pdf. Accessed 8 Mar 2012
38. FoeBuD e.V. Die StopRFID-Seiten des FoeBuD e.V. (2012), http://www.foebud.org/rfid/index_html. Accessed 8 Mar 2012
39. M. Abadi, C. Fournet, Access control based on execution history, in *Proceedings of the 10th Annual Network and Distributed System Security, Symposium* (2003), pp. 107–121
40. G. Edjlali, A. Acharya, V. Chaudhary, History-based access control for mobile code, in *Proceedings of 5th Conference on Computer and Communications, Security* (1998), pp. 38–48

http://www.springer.com/978-3-642-36342-9

Real-time Security Extensions for EPCglobal Networks
Case Study for the Pharmaceutical Industry
Schapranow, M.-P.
2014, XXII, 146 p., Hardcover
ISBN: 978-3-642-36342-9