Security Challenges of the EPCglobal Network

Benjamin Fabian and Oliver Günther
Humboldt-Universität zu Berlin
Institute of Information Systems
(bfabian, guenther)@wiwi.hu-berlin.de

The “Internet of Things,” once reality, will have to rely on a global IT infrastructure that provides information about all those “things” in a secure and reliable manner. The EPCglobal Network is a proposal for a widely distributed information system to offer such services. But it may offer more transparency than was initially anticipated.

Introduction

If the vision of many RFID proponents becomes true, more and more common objects will soon acquire a cyber presence. Objects will be equipped with RFID tags containing identification data and possibly some additional information about the object in question (“data on tag”). To keep tag costs low, one may often just store an identifier and use it as a key to access databases containing the actual object information (“data on network”).

This second approach is typical for “EPC tags” – RFID tags that aim to replace the conventional barcode system. They use an Electronic Product Code (EPC, see Figure 1), which is globally unique, as a key to retrieve information from the EPCglobal Network, a large distributed system of databases [12]. The EPC standard represents a numbering framework that is independent of specific hardware features, such as tag generation or specific radio frequency.

The object databases of the EPCglobal Network are run by manufacturers, logistic providers, retailers, or third parties, and can be accessed via special web services called EPC Information Services (EPCIS). The network architecture is designed and administered by the standardization consortium EPCglobal, which is a joint venture of GS1 US (formerly Uniform Code Council) and GS1 (EAN International).

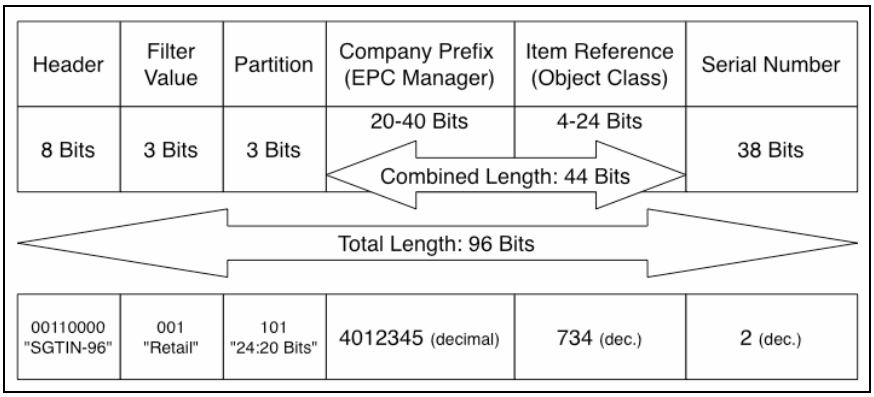

Figure 1: Example of an Electronic Product Code (SGTIN-96 EPC)

By improving the information flow, as objects pass from suppliers to manufacturers, distributors, retail stores, and customers, the EPCglobal Network aims to facilitate cooperation within supply chains and thus to make them more effective. Once established, it could also be used to support a wide range of applications in the area of Ubiquitous Computing (UC). An often-cited example is the "smart home" [6], in which "intelligent" cupboards and fridges could be realized using RFID technology. By scanning the RFID tags on objects and using the EPCglobal Network for information retrieval, such devices can identify their current content and offer new services like food counseling or automated replenishing of goods.

As a result of this broadened use of the EPCglobal Network, its security context will change from closed supply chains to the rather open environments of UC – like the security context of the Internet and the Web was changed by moving from relatively closed groups of fellow researchers to the global environment it represents today. Interestingly, until today there is no public official document discussing the security and privacy requirements of the EPCglobal Network in depth, neither for supply chains, nor for UC and home applications.

In this article, we first describe the EPCglobal Network architecture, as it is specified by current design drafts. We then discuss its security and privacy risks, as well as possible countermeasures. We conclude with suggestions on how to improve existing design proposals, once appropriate security and privacy requirements have been established.

The EPCglobal Network Architecture

To cope with dynamic data flows on a truly global scale, the EPCglobal Network allows all relevant parties (manufacturers, suppliers, shops, after-sale service providers) to dynamically register EPC Information Services. This enables the flexible exchange of information about the products they are concerned with.

In order to locate these dynamically registered EPCIS, a static list or a single server would lead to out-of-date information and scalability problems. The EPCglobal Network therefore includes central look-up services called EPCIS Discovery Services and Object Naming Service (ONS) [12]. Each time someone requests information about a particular object (not already present in local caches, or "stale"), these services are queried for a recent list of relevant EPCIS. After retrieving this list, the requestor directly contacts the EPC Information Services he or she is interested in.

Thus, object information retrieval in the EPCglobal Network generally consists of three main phases (cf. Figure 2):

1. *RFID Tag-to-Reader and Intranet Communication:* An RFID reader reads an EPC from an RFID tag via wireless communication (1a). This EPC is transmitted to a middleware layer for further processing (1b).
2. *EPCIS Discovery and ONS:* This phase will involve EPCIS Discovery Services that are not specified yet [12] (2a). According to [10], the middleware queries ONS for Uniform Resource Locators (URLs) of corresponding information sources (EPCIS) [10] (2b). The final answer (2c) from the Local ONS of an information provider is handed over to the application (2d).

3. *EPCIS Access:* The application needs to resolve the EPCIS DNS names (3a, b) delivered by ONS, and finally contacts the relevant EPCIS directly to retrieve the object information (3c).

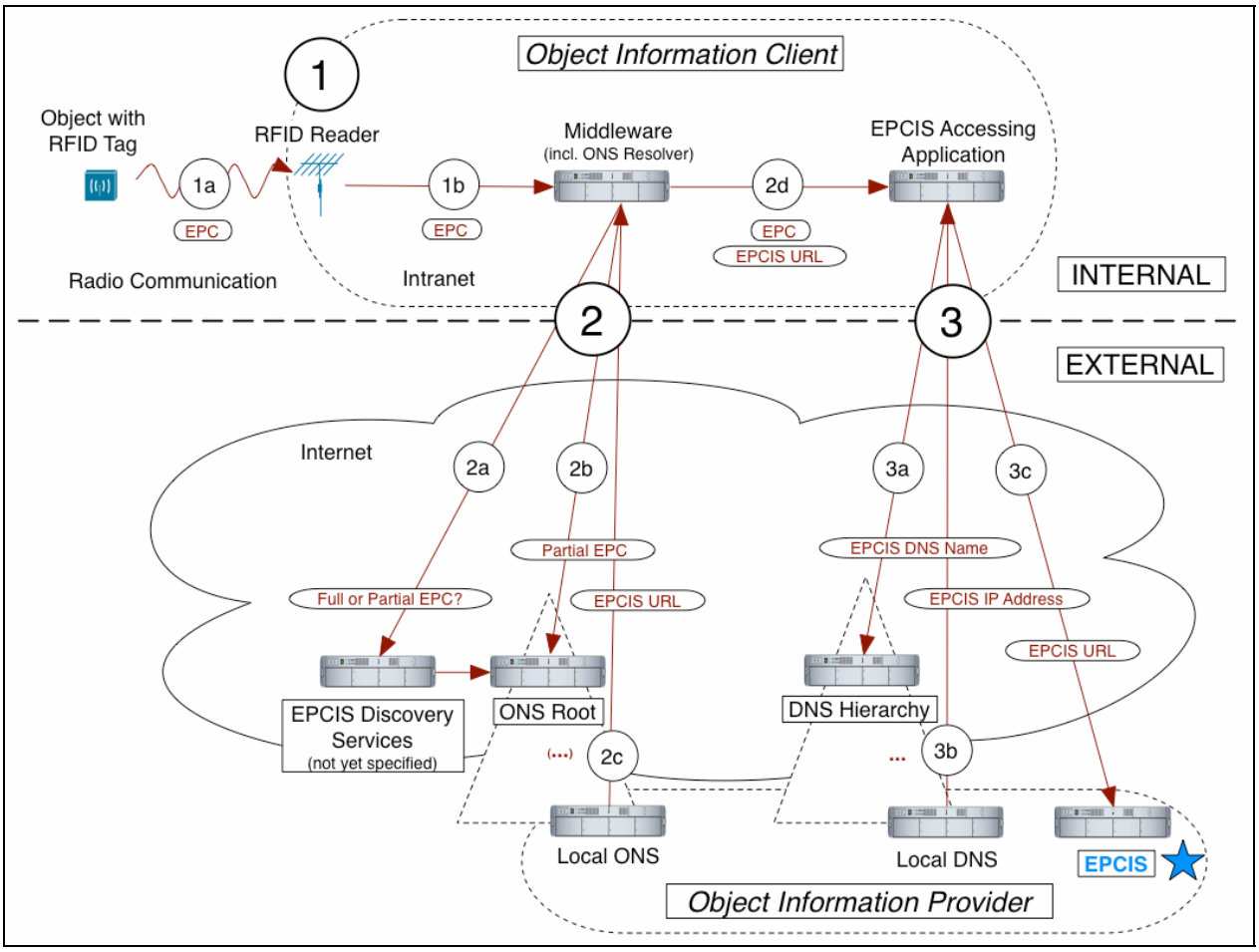

Figure 2: Example Communication Flow in the EPCglobal Network

Risks

From a privacy and security perspective, each of these phases presents specific challenges [4]. Phase 1, especially the tag and reader radio communications (1a), has so far caused most concerns in the public conscience [5]. Though the current EPC tags (UHF Class 1 Generation 2) are equipped with some basic security functions, they do not offer access control for the EPC, only for additional data on the tag [12]. Limited tag capabilities have inspired much research on light cryptography (for a survey see [8]).

Concerning phase 2, the inner workings of EPCIS Discovery Services (2a) are not public as of yet. But ONS resolution (2b,c) brings about enough hard security challenges in its current design. Before we discuss these in detail, we take a closer look at the inner workings of ONS.

Technically, ONS is a subset of the Domain Name System (DNS). The idea is to first encode the EPC into a domain name while preserving its structure and field values (e.g.,

734.4012345.sgtin.id.onsepc.com for the EPC in Figure 1), then to use the existing DNS protocol and delegation procedures. The current ONS specification states that the serial number of the EPC (which differentiates items of the same kind, like two watches of the same model and manufacturer) should not be used for delegation, but leaves room for future extensions [10].
Using DNS for ONS implies a potentially dangerous heritage [4]. DNS is a central Internet service with a long history of security issues with respect to the protocol itself and its implementations [11]. A detailed threat analysis is given in [1]. Some of the threats target availability (denial of service), others integrity of DNS information (cache poisoning, Man-in-the-Middle attacks). DNS, as it is commonly deployed, has no way of authenticating communication partners or the information that is provided. Further, DNS is a clear text protocol, which is necessary to use parts of a domain name for delegation purposes (2b,c). These weaknesses directly transfer to ONS if no additional countermeasures are implemented and create risks on a new scale for processes relying on a secure "Internet of Things".

In phase 3, the initial standard DNS lookup (3a,b) is subject to similar threats as the ONS resolution. Authentication and encryption of the EPCIS connection (3c) could be achieved by using common security protocols. However, EPCIS access involves additional risks for privacy, too.

Confidentiality and Privacy. There are many situations where the EPC stored on an RFID tag should be regarded as sensitive information – be it in a private context [5], where people fear to be tracked or have their belongings read out by strangers, or in a business context, where product flows constitute valuable business intelligence.

The combination of an EPC company identifier and item reference is usually enough to determine the exact kind of object it belongs to. This information can be used to identify assets of an individual or an organization. If somebody happens to wear a rare item or a rare combination of belongings, one could track that person even without knowing the actual serial numbers (Cluster Tracking). For an overview of possible inferences from query data, see Table 1.

Query Data	**Inferable Information**	**Possible Adversary Analysis**
Source IP Address, Time	Identity and location of the information client. Frequency of objects passing RFID readers.	Who does the query? Where is she located? At what time and how often are items used or processed?
EPC Company Prefix	Manufacturer	What general brand is used? High-level consumer preferences. Tracking of very rare brands.
EPCIS DNS Name	Manufacturer	"
EPCIS IP Address	Manufacturer	"
EPCIS URL	Manufacturer	See above, plus analysis using EPCIS directory structure.
Partial EPC (= Company Prefix + Item Reference)	Manufacturer. Object class.	Exact item category of this brand. Detailed consumer preferences. Rare item or Cluster Tracking.
EPC (= Partial EPC + Serial Number)	Unique object identity.	Which unique item within this kind and brand? Detailed consumer

		preferences and buying behavior. Identity of object owner or holder. Social or business networks.
Unencrypted EPCIS Reply Content	Object information related to this EPC.	Depends on specific content.

Table 1: Privacy and Confidentiality Risks

To retrieve the information stored in the EPCglobal Network about a given EPC, it is necessary to locate the corresponding EPCIS servers first. Because the EPC structure is used for delegation, it is not easily possible to use encryption in this phase.

Thus, the partial EPC (consisting of Company Prefix and Item Reference) will first traverse local area networks (LAN), potentially involving insecure wireless networks. A local network sniffer, however, could potentially also capture the complete EPC from other Intranet messages (1b, 2d).

Depending on the actual configuration of ONS caching, this partial EPC will also be transmitted to external ONS on the Internet in clear text. This process always starts at the Root ONS [12]. Finally, the query reaches the Local ONS (3b) server of the manufacturer. All queried servers and Internet service providers (ISP) on the path could capture and store the partial EPC, as well as the origin (source IP address) of the query. For a very general classification of potential adversaries in terms of user coverage see Figure 3.

Even if the actual connection to an EPCIS server (3c) is encrypted, the EPCIS operator himself (e.g., the manufacturer) could compile profiles of the subset of EPCglobal Network users who query for information at this particular server. The initial DNS lookup (3a) could betray the object brand to an even larger set of adversaries.

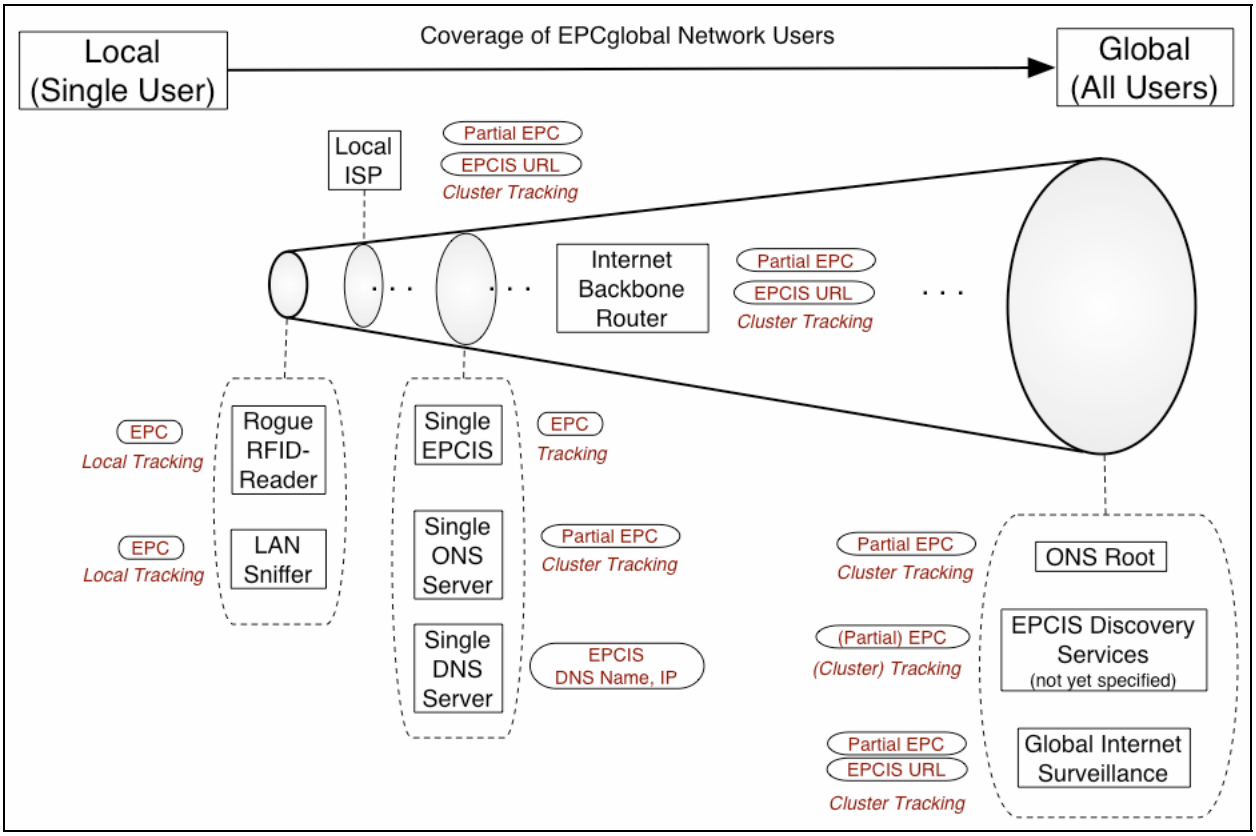

Figure 3: User Coverage of Different Adversary Models

Integrity. In the EPCglobal Network, integrity refers to the correctness and completeness of the returned ONS information, in particular the addresses of the relevant EPCIS, and the object information itself (we subsume authenticity here). Attackers who control intermediate ONS or DNS servers, or launch a successful man-in-the-middle attack on the communication could forge the returned list of EPCIS and include, for example, a server under their control. Many problematic situations could result from such a security breach. Just imagine, for example, that the query was issued by a smart medicine cabinet to prevent harmful drug mixes, or by a business IT system to locate special servers for detecting product counterfeits.

Availability. If the EPCglobal Network becomes widely accepted, more and more business processes (B2B, B2C), as well as personal applications, will be able to use it without human intervention. This would leave these processes highly dependable on a working EPC resolution service for finding matching information sources. An EPCIS, as well as ONS, constitutes a service highly exposed to attacks from the Internet due to its necessary accessibility. This includes distributed denial-of-service attacks overwhelming the server by issuing a large number of queries, or targeted exploits. Therefore, an integration of the EPCglobal Network (as proposed) into core business processes would increase the dependency of corporations on the Internet and their operational business risk.

Countermeasures and Their Effectiveness

In the following, we discuss some countermeasures to mitigate the indicated risks. For a preliminary and very general evaluation of their effect and practicality, see Table 2. Some of these methods could be combined to create alternatives to the current EPCglobal Network design.

Counter-measure	**Security and Privacy**				**Practicality**	
	Anonymity	Confidentiality	Integrity	Availability	ONS	EPCIS
VPN		+	+		-	-
TLS		+	+		-	+
DNSSEC			+			
Mixes	+	(+)	(+)		-	
PIR	+	+	(+)		-	-
P2P	(+)			+	+	+

Table 2: General Effectiveness of Countermeasures

VPN. Closed groups of business partners who run a private version of the EPCglobal network may be able to reduce their confidentiality and integrity risks by using extranets over Virtual Private Networks (VPN). This solution, however, would not scale to the general case of a dynamic global exchange, given the known scalability issues and administrative overhead associated with VPN.

TLS. Using Transport Layer Security (TLS) could solve problems of EPCIS confidentiality and integrity if an appropriate global trust structure could be established, but it would negatively affect the performance of the ONS look-up process.

DNSSEC. An approach to address security shortcomings of DNS is called DNS Security Extensions (DNSSEC). It provides mutual authentication between DNS servers by using shared secrets, as well as origin authenticity and data integrity (but explicitly no confidentiality, cf. RFC 4033) for the delivered information by public-key cryptography. DNSSEC has not been widely adopted so far. Reasons for this include scalability problems of key management, difficulties in building chains of trust between servers of many different organizations, and the crucial question who should control the root of trust. Finally, reasonable reservations exist to touch a running critical system, because many IT applications depend on DNS in unexpected ways [9]. DNSSEC could assure ONS information authenticity on a global scale if the Internet community as a whole adopts it. Otherwise, membership in the EPCglobal Network would remain small, and its impact on global information exchange be greatly diminished.

Anonymous Mixes. The key idea of anonymous mixes and onion routing (such as TOR [3]) is to cryptographically transform and mix Internet traffic from many different sources, in order to hamper matching a particular IP packet to a particular source. For ONS, usability would be reduced by latency and performance issues. Such approaches could also be used to anonymize traffic directed at EPCIS servers, and would be viable also for private households. This could enhance anonymity and perhaps confidentiality, but not the integrity of the received messages. In addition, conflicts between anonymity and identification needs for EPCIS access control will need to be solved.

Private Information Retrieval. Methods from Private Information Retrieval (PIR) [7] could in principle be implemented to obfuscate which client has interest in exactly what information, once the EPCIS have been located. But in the case of a globally distributed look-up system (like ONS), problems of scalability and key management, as well as performance issues, seem to render this approach impractical.

Peer-to-Peer Systems. Decentralized alternatives to classical network service architectures exist in the form of Peer-to-Peer Systems (P2P), especially structured P2P systems using distributed hash tables (DHT) [2]. They offer robustness to faults, avoid single points of failures (e.g., they have no single root like DNS), and distribute load among participants more evenly. With ongoing projects like CoDoNS [11] that build alternatives to classical DNS, ONS and EPCIS could also be based on DHT. Just using a P2P architecture, however, does not guarantee integrity and confidentiality, and only slightly enhances anonymity (by increasing the number of nodes to be monitored).

Conclusions

Like in the case of RFID wireless communication, true security is sorely lacking in the design of the EPCglobal Network and especially the ONS so far. It is likely that the final design of the EPCglobal Network will include some kind of central certificate authority (CA) [12]. How scalable this will turn out in real applications, remains unclear. Moreover, such a CA would constitute another single point of failure and would have to be trusted by all current and future parties involved. The forthcoming EPCIS Discovery Services should be designed carefully, as they are about to infer huge privacy risks (global coverage, possible transfer of the full EPC).

Instead of adding another level of functionalities to the already burdened and insecure DNS, implementing an “Internet of Things” should be regarded as an opportunity to phase in new technologies (such as P2P) into the Internet infrastructure.

Before deploying systems at a global scale that have a possible impact as *de facto* standard for years to come, it is essential to perform a thorough analysis of multilateral security and privacy requirements, involving the current and potential future stakeholders. As we have learnt with the Internet, adding security as an afterthought is usually a very bad idea.

References

1. Atkins, D., and Austein, R. Threat Analysis of the Domain Name System (DNS). Request for Comments (RFC) 3833, 2004.
2. Balakrishnan, H., Kaashoek, M. F., Karger, D., Morris, R., and Stoica, I. Looking up Data in P2P Systems. Commun. ACM, 46(2), 2003, 43–48.
3. Dingledine, R., Mathewson, N., and Syverson, P. TOR: The Second Generation Onion Router. Proceedings of the 13th USENIX Security Symposium, August 2004.
4. Fabian, B., Günther, O., and Spiekermann, S. Security Analysis of the Object Name Service. Proceedings of SecPerU 2005 in conj. with IEEE ICPS 2005 (Santorini, Greece), 71–76.

5. Günther, O. and Spiekermann, S. RFID and the Perception of Control: The Consumer's View. Commun. ACM, 48(9), Sept. 2005, 73–76.
6. Helal, S., Mann, W., El-Zabadani, H., King, J., Kaddoura, Y., and Jansen, E. The Gator Tech Smart House: A Programmable Pervasive Space. IEEE Computer Magazine, March 2005, 50–60.
7. Iliev, A. and Smith, S. W. Protecting Client Privacy with Trusted Computing at the Server. IEEE Security and Privacy, 3(2), March-April 2005, 20–28.
8. Juels, A. RFID Security and Privacy – A Research Survey. IEEE Journal on Selected Areas in Communications, 24 (2), Feb. 2006, 381–394.
9. Kaminsky, D. Explorations in Namespace: White-hat Hacking across the Domain Name System. Commun. ACM, 49(6), June 2006, 62–69.
10. Mealling, M. EPCglobal Object Naming Service (ONS). EPCglobal Ratified Specification, Version 1.0, 2005; www.epcglobalinc.org/standards/.
11. Ramasubramanian, V. and Sirer, E. G. The Design and Implementation of a Next Generation Name Service for the Internet. Proceedings of SIGCOMM '04. ACM Press, 2004, 331–342.
12. Traub, K. (ed.): The EPCglobal Architecture Framework, Final Version, July 2005; www.epcglobalinc.org/standards/.