Comparison of DNSSEC and DNSCurve securing the Object Name Service (ONS) of the EPC Architecture Framework

Rosenkranz, Demian, University of Applied Sciences Bonn-Rhein-Sieg, 53757 Sankt Augustin, Germany
Dreyer, Mark, University of Applied Sciences Bonn-Rhein-Sieg, 53757 Sankt Augustin, Germany
Schmitz, Patrick, University of Applied Sciences Bonn-Rhein-Sieg, 53757 Sankt Augustin, Germany
Schönborn, Johannes, University of Applied Sciences Bonn-Rhein-Sieg, 53757 Sankt Augustin, Germany
Sakal, Peter, University of Applied Sciences Bonn-Rhein-Sieg, 53757 Sankt Augustin, Germany
Pohl, Hartmut, University of Applied Sciences Bonn-Rhein-Sieg, 53757 Sankt Augustin, Germany

Abstract

Using the Electronic Product Code (EPC) in the future mostly stored on a Radio Frequency Identification (RFID)-chip, it is possible via e.g. the ONS of the EPC Architecture Framework to distinguish each item worldwide and to trace it back in the supply chain to the producer and furthermore to the subcontractors. The paper describes the comparison of two mechanisms with different security goals to improve the trust level of ONS: DNSSEC and DNSCurve. DNSSEC enables integrity and authenticity - DNSCurve additionally enables confidentiality and a higher availability. The necessary manpower to install DNSCurve is much lower compared to DNSSEC.

1 Challenges

The project Trusted EPC Administration (TEA)[1] has been working on the problems and challenges discussing the trusted global tracking of products along the supply chain since 2009. Last year the team of TEA published a paper [1] which explained and rated the options to increase the security level in the RFID based supply chain. In this paper the focus is the comparison of two possible DNS security extensions. The following scenario has been secured: A customer purchases a small bottle of an often faked medicine (e.g. Viagra®) in a pharmacy and wants to verify its originality immediately. He presents the bottle to a RFID-reader inside the pharmacy, which sends the acquired data using the internet to the Object Naming Service (ONS), Discovery Service (DS) and EPC Information System (EPCIS). First of all the customer asks for confidentiality of the communication (his name etc.), furthermore he asks for anonymity against the producer and is interested to get an answer with integrity. The producer asks for authenticity because he doesn't want to answer to counterfeiters spoofing correct product numbers (EPC).

2 Prototype

2.1 EPC Architecture Framework

To allow tracking of products storing an unique EPC, an open and supplier-neutral architecture which provides a worldwide and cross-company solution is necessary. The EPC Architecture Framework (Figure 1) provides a platform independent configuration of hardware, software and data standards.

The previously mentioned example of the product Viagra® illustrated on this framework outlines the process involved components of the framework. In this case the starting point in the figure would be the subscriber (customer, consumer). A consumer owns a product with an unique EPC stored on a RFID-chip. Now the consumer checks the authenticity of his product using a terminal in the pharmacy. Using a RFID-reader he scans the EPC of his product and starts sending a query to the ONS via the terminal. Trusted operating environment of the terminal i.e. protecting from radio frequency emission is assumed. The ONS receives the EPC and looks for the related EPCIS of the manufacturer. The terminal receives the address of the EPCIS and contacts the EPCIS directly with a query containing the EPC of the product. Now the EPCIS of the manufacturer can check whether the requesting user at the terminal is a certain consumer, merchant, supplier, partner, anonymous etc. and as a result the EPCIS sends the specific information for the user back to the terminal. Eventually the consumer gets the information whether the EPC of his product is valid or a fake. To allow anonymous requests, not every consumer must has a certificate, but in this case the consumer has only limited EPCIS functionality - according to the access control policy (ACP).

Every interface marked as a (optional) security service and every communication path between two incident security services is a possible attack surface and must be provided with suitable services which secure the communication and raise the resistance against attacks [4]. By ACP the producer must be enabled to configure his EPCIS to only send approved information to a subscriber. However, for the ONS itself an ACP is not necessary, as the ONS owns no information except the address of the producer. This enables the consumer to start an anonymous query to the

[1] Sponsored by the German Federal Ministry of Education and Research No. 01 IS 08043B

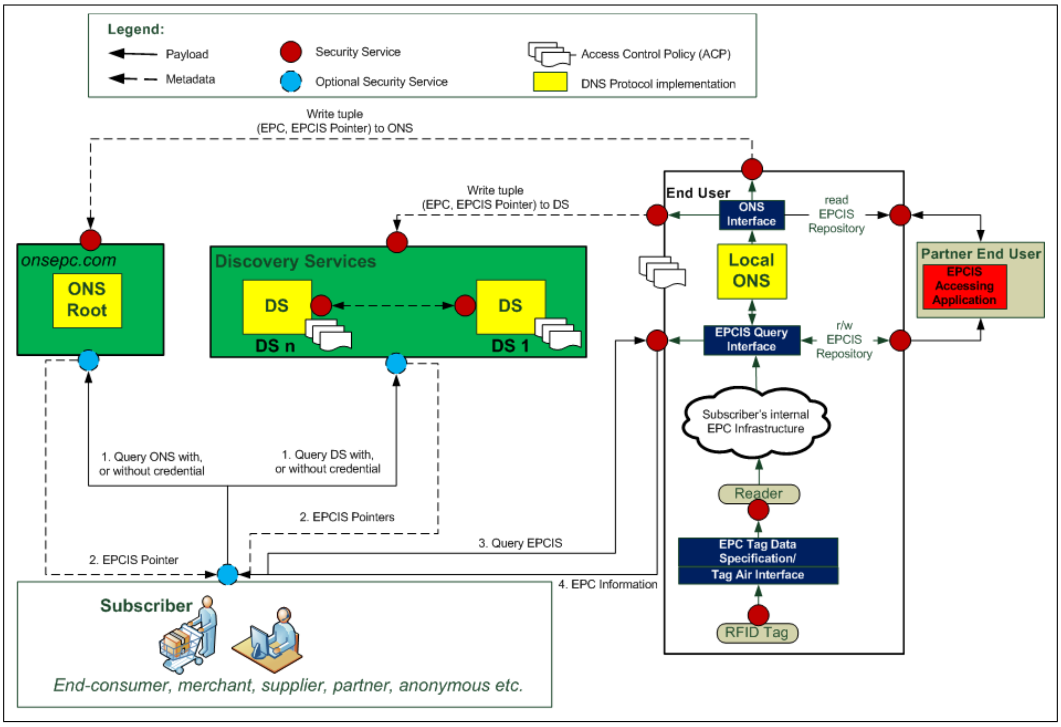
Legend:
Payload
Metadata
Security Service
Optional Security Service
Access Control Policy (ACP)
DNS Protocol implementation
Write tuple (EPC, EPCIS Pointer) to ONS
Write tuple (EPC, EPCIS Pointer) to DS
End User
ONS Interface
read EPCIS Repository
Local ONS
Partner End User
EPCIS Accessing Application
onsepc.com
ONS Root
Discovery Services
DS
DS n
DS
DS 1
EPCIS Query Interface
r/w EPCIS Repository
Subscriber's internal EPC Infrastructure
1. Query ONS with, or without credential
1. Query DS with, or without credential
Reader
2. EPCIS Pointers
3. Query EPCIS
EPC Tag Data Specification/ Tag Air Interface
2. EPCIS Pointer
4. EPC Information
Subscriber
RFID Tag
End-consumer, merchant, supplier, partner, anonymous etc.

Figure 1 Security Services in EPC Architecture Framework

ONS and prevents the connection between customer and product to be known.

2.2 Query Front-end

The Query Front-end of the prototype of TEA is a graphical web-based user interface. Authorized subscribers have to validate themselves towards the EPCIS by certificates generated by a Public Key Infrastructure (PKI) [2] in order to receive specific information about a product provided with an EPC. This allows a software-based solution for the prototype.

2.3 Object Name Service

The Object Name Service (ONS) works like the well-known Domain Name System (DNS). It starts with the resolution of a query, in this case for an EPC, and ends with the answer from the resolution in form of an address of an EPCIS related to the EPC. The essential difference compared to the DNS is that the ONS owns in each case only one address to a possible query based on an EPC and sends it as an answer. Because the functionality and the requirements of both ONS and DNS are identical, the use of DNS-software is obvious.

3 Securing DNS

In the past two years, the Domain Name Service (DNS) was repeatedly attacked mainly by cache poisoning [12] - a denial of service - accomplishing attacks [11].

The implementation of the ONS inside the EPC Architecture Framework is based on DNS. On account of this at least the security goals confidentiality, authenticity and integrity have to be achieved by the ONS. As DNS itself does not suffice the demands of the TEA project (confidentiality, integrity, availability, authenticity/non-repudiation), several technologies to improve the security standard of DNS have been created.

Table 1 shows the currently most important technologies and their representative protective goals.

Mechanism	AT	CF	IN
DNSSEC	*		*
DNSEC using NSEC	*		*
DNSSEC withNSEC3	*		*
TSIG	*		*
TKEY and SIG(0)	*		*
DNSCurve	*	*	*

Table 1 Securing DNS

Legend:
AT –> Authenticity, CF –> Confidentiality, IN –> Integrity

In the following, Domain Name System Security Extensions (DNSSEC) and DNSCurve will be discussed.

3.1 DNSSEC

DNSSEC guarantees the protective goals authenticity and integrity for ONS information. Additional to the known resource records (RR) DNSSEC uses specific resource records. DNSSEC applies an asymmetric pair of keys (zone signing keys) to each secured zone. Each RR will be signed using the private zone key. The signature of one or more RR of the same type will be deposited in a signature resource record. DNSSEC is capable to use the algorithms RSA[2]/Secure Hash Algorithm 1 (SHA-1), Digital Signature Algorithm (DSA)/SHA-1 and RSA/Message-Digest Algorithm 5 (MD5). MD5 is not longer recommended because of the insecure MD5 hash algorithm [5].

The implementation of DNSSEC required significant changes in the configuration of the nameserver. Larger compounds of the zone file have to be changed or complemented. Among these comes the integration of the key signing keysand the zone signing keys.

3.2 DNSCurve

The product suite DNSCurve [16] is based on the special elliptic curve Curve25519. DNSCurve can be used to achieve integrity, authenticity and confidentiality for ONS information. By using DNSCurve the content of transmitted and received data packets are neither unrecognized modified nor readable for attackers using encryption and digital signatures.

Only a patched forwarder on the server side and a patched DNS-cache on the client side is needed (Figure 2). These components have to be integrated between DNS server and client to handle the incoming and outgoing requests.

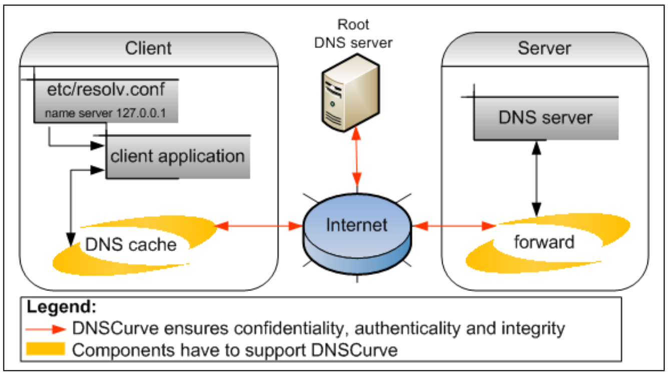

Figure 2 Communication in DNSCurve

Encryption and the key sharing process of DNSCurve is known as Two Key Communication [13] [14]. Additionally - as for asymmetric encryption common - hash keys will be compared to ensure integrity.

4 Comparison

4.1 Installation effort

Two reasons for the slow circulation of DNSSEC are the high administrative effort and the involved costs within the adoption and maintenance. An error-prone migration to DNSSEC might jam whole zones in result.

Until today many home office and small office routers are not able to compute DNSSEC queries larger than 512 Byte (UDP) and simply drop them without notifying the user [9]. This is a limiting factor for the integration of DNSSEC in a network like the EPC Architecture Framework.

For this is a known problem a testbed has been established in Germany to promote the acceptance of DNSSEC. It is supported by "Deutsches Network Information Center" (DENIC) - the manager of top-level domain for Germany [7].

DNSCurve is currently the most important competitor of DNSSEC. DNSCurve allows an easy integration because of its black box architecture and requires only a small amount of maintenance costs. Also small office and home office routers can handle the encrypted content of the DNSCurve packets [9].

There is only a prototype implementation of DNSCurve available at the moment. A date for a stable version of DNSCurve is not known. The release of a stable version of DNSCurve is mandatory for its use within the EPC Architecture Framework.

4.2 Protective goals

Both DNSSEC and DNSCurve ensure the protective goals authenticity and integrity. In contrast to DNSCurve, DNSSEC does not provide confidentiality. In a network like EPC Architecture Framework that communicates sensitive data, confidentiality is essential [3]. The consequence is, that ONS secured by DNSSEC can't serve the confidentiality for the customer (subscriber). This gets emphasised by the example of the customer who wants to buy Viagra®. The customer has to be anonym against the manufacturer. Furthermore no third party may get the chance to attain these information.

Contrary to DNSCurve DNSSEC requires the zone signing keys (ZSK) and key signing keys (KSK) to be updated in a certain interval. In this context the KSK is responsible for the proof of identity. The renewal of the KSK is critical as a breach of security might cripple a whole zone [8].

Another important aspect of DNSSEC is the usage of the RSA-1024 as encryption of the root zone [10], which - in consideration of major botnets [17] - does not provide sufficient trust level. RSA-1024 might be already broken (i.e. by larger companies or botnets) [15]; but until today there is no scientific verification. Using DNSSEC the EPC Architecture Framework might be compromised.

DNSCurve uses Curve25519 which is efficient and applies

[2] stands for Rivest, Shamir and Adleman who first publicly described it

Query	DNS	DNSSEC	DNSCurve
Existent domains	119 bytes (100%)	341 bytes (287%)	304 bytes (255%)
Non-existent domains	-	697 bytes	-

Table 2 Average size of response packets [5]

a high security level: A similar level of security is possible with 3000-bit RSA, but encryption and authentication with 3000-bit RSA is not fast enough to handle modern DNS loads and would require much more space in DNS packets [16].

4.3 Performance and scalability

To ensure not only security but also scalability in the EPC Architecture Framework dealing with enormous amounts of traffic, a high performance encryption algorithm has to be applied. Using DNSSEC increases the size of the response packets enormously because of the additional Resource Records (RR) sent. To illustrate the difference in size, different signed and unsigned DNS requests were sent to the server. The names of the requested domains had an average length of ten characters. The zone signature had a length of 1024 Bit. Table 2 illustrates the average size of the response packet.

The size of DNSCurve packets is larger in comparison to standard DNS packets. During the sample requests, size of DNSCurve packets rose by 255%. Using DNSSEC increases packet size by 287%. It remains to note that DNSCurve achieves more protection goals (cf. table 1) then DNSSEC while getting along with smaller packet size. This can be traced back to the shorter encryption keys of DNSCurve which results of the use of Elliptic Curve Cryptography (ECC). Furthermore DNSCurve and standard DNS do not generate traffic when requesting a non-existing domain, while DNSSEC does (cf. table 2) [5].

According to Prof. Bernstein - the originator of DNScurve - about 50 billion DNS packets are sent within the .com zone each day. The application of DNSSEC would increase the anyway enormous traffic significant. This is counted to the 287% increased packet size compared to DNS and additionally sent response packets when requesting non-existent domains [5]. Using DNSSEC to secure the ONS of the EPC Architecture Framework which handles world wide requests would also increase the traffic significant.

The advantage in performance of DNSCurve is shown in table 3. 10.000 pairs of keys have been computed, using RSA, DSA and ECC. Table 3 shows the mean time measured in seconds needed to compute the belonging keys. To minimize discordant values, three different CPU architectures Intel Centrino Duo, Athlon X2 and Intel i7 920 were used to calculate the mean time for computing the keys.

Time measured in s		
RSA	DSA	ECC
377.06	32.77	33.71

Table 3 Benchmark for RSA, DSA and ECC

The calculation of DSA and ECC keys is significant faster as the calculation of RSA keys. DSA and ECC needed a similar length of time to compute the keys, but a RSA and DSA key length of 1024 Bit corresponds to an ECC key length of 160 Bit at comparable trust level. ECC Curve prime 192v1 has been used to compute the ECC equivalent. Therefore the ECC algorithm outperforms RSA and DSA by a factor of almost 10 [6]. In view of the performance the use of DNSCurve in ONS as a component of the EPC Architecture Framework is recommended instead of DNSSEC.

5 Summary

The use of DNS was not to be recommended up to now if a high security level had to be guaranteed e.g. in the EPC Architecture Framework. Therefore, this paper has been compared two possible solutions for securing DNS. Table 4 summarizes the main findings from the comparison of DNSSEC and DNSCurve.

		DNSSEC	DNSCurve
Installation effort	Router problem	Yes	No
	Nameserver configuration changes required	Yes	No
Protective goals	Authenticity	Yes	Yes
	Confidentiality	No	Yes
	Integrity	Yes	Yes
Performance	Packet size	Larger	Lower
	Performance at minimum same security level	Higher	Lower

Table 4 Summary of DNSSEC and DNSCurve

DNSSEC does not implement confidentiality. The use of RSA 1024 is insecure and common routers might not be able to process encrypted packets. Using DNSCurve to ensure the security goals authenticity, integrity and confidentiality enables the domain name service in the future to be used in environments where a high security level has to be guaranteed, i.e. ONS.

6 References

[1] Sakal, P., Iltisberger, B., Stein, T., Hastrich, M., Pohl, H.: Trusted EPC Administration. Bremen 2009.

[2] Pohl, H., Wallstabe, A.: Implementing high-level Counterfeit Security using RFID and PKI. Duisburg 2007 - http://www.inf.fh-bonn-rhein-sieg.de /data/informatik/fb_informatik/personen/pohl/Aufsaetze/Pohl_Wallstabe_High_Level_Counterfeit_ Security_2007_.pdf.

[3] Pohl, H. et al.: Bewertung des Sicherheitsniveaus einiger Mechanismen zur Vertraulichkeit, Verfügbarkeit und Pseudonymität von Transpondern (RFID). Darmstadt 2006 - http://www.fh-brs.de /informatikmedia/Downloads/Personen/pohl/Aufsaetze/Pohl_Jung_Roth_Bewertung_des_ Sicherheitsniveaus_von_Transpondern_.pdf.

[4] Knospe, H., Pohl, H.: RFID Security. Information Security Technical Report. 2004 - http://www.inf. fh-bonn-rhein-sieg.de/data/informatik_/fb_informatik /personen/pohl/Aufsaetze/Pohl_Knospe_RFID_ Security_050126.pdf.

[5] Wörner, E. (Ed.): Sicherheit von DNS. 2009 - http:// www.informatik.uni-augsburg.de/de/lehrstuehle/swt /se/teaching/ss09/internetsicherheit/Downloads/DNS-Ausarbeitung.pdf.

[6] Gura, N., Patel, A., Wander A., Eberle H., Chang Shantz, S. (Ed.): Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs. 2004.

[7] DENIC (Ed.): DNSSEC - Testbed für Deutschland. 2009 - http://www.denic.de /fileadmin/Domains/DNSSEC/DNSSEC_Testbed_ fuer_Deutschland.pdf

[8] Heise (Ed.): Router-Inkompabilität. Hannover 2010 - http://www.heise.de/netze/artikel/DNSsec-Router-Inkompatibilitaet-903752.html.

[9] Heise (Ed.): BSI-Studie: Viele Heimrouter beherrschen kein DNSsec. Hannover 2010 - http://www.heise.de/security/meldung/BSI-Studie-Viele-Heimrouter-beherrschen-kein-DNSsec-914777.html.

[10] Heise (Ed.): Erster Root-Server liefert ab 1. Dezember DNSSEC-signierte Zone. Hannover 2009 - http://www.heise.de/security/meldung/Erster-Root-server-liefert-ab-1-Dezember-DNSSEC-signierte-Zone-814252.html.

[11] Heise (Ed.): USA: Attacke auf DNS-Anbieter stört Online-Weihnachtsgeschäft. Hannover 2009 - http://www.heise.de/security/meldung/USA-Attacke-auf-DNS-Anbieter-stoert-Online-Weihnachts-geschaeft-892686.html.

[12] Heise (Ed.): DNS-Vergifter entführen Tippfelher-Domains. Hannover 2008 - http://www.heise .de/security/meldung/DNS-Vergifter-entfuehren-Tippfelher-Domains-198527.html.

[13] Bernstein, D.: Curve25519: new Diffie-Hellman speed records. 2006 - http://cr.yp.to /ecdh/curve25519-20060209.pdf.

[14] Bernstein, D.: Cryptography in DNSCurve. 2009 - http://DNSCurve.org/crypto.html, 25.08.2009.

[15] Bernstein, D.: DNSCurve - DNS forgery. 2009 - http://dnscurve.org/forgery.html, 25.08.2009.

[16] Bernstein, D.: Website DNSCurve Project. 2009 - http://www.dnscurve.org, 25.08.2009.

[17] F-Secure (Ed.): Calculating the Size of the Downadup Outbreak. 2009 - http://www.f-secure .com/weblog/archives/00001584.html, 25.08.2009.

[18] Markoff, J.: Worm Infects Millions of Computers Worldwide. 2009 - http://www.nytimes.com/2009/01/ 23/technology/internet/23worm.html?_r=1, 25.08.2009.

[19] Schmeh, K.: Kryptographie - Verfahren, Protokolle, Infrastrukturen. Heidelberg 2009.