Standardization of Privacy and Trust Enhancing Technology Projects

Cyrill Krähenbühl
Adrian Perrig

June 14, 2020

This documentation offers guidance about software standardization of privacy and trust enhancing technology from the Network Security Group of ETH Zürich [1]. The content was organized for technology projects funded by the Next Generation Internet R&D initiative [2], specifically the NGI Zero PET [3] grant program for privacy and trust enhancing technology. The content can also help readers more generally interested or involved in standardizing privacy and trust enhancing technology.

Contents

1 Standardization Overview

A standard is defined by the European Telecommunications Standards Institute (ETSI) as "a document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context". [4]

When it comes to standardization, there are three central questions that have to be answered. The first question is about the motivation of producing a standards document for a specific protocol or technology. Is the protocol being used by people or machines that are not managed by a single entity, e.g., not within the same corporate network? Is the protocol not proprietary or are there publicly available implementations, e.g., competing implementations by different vendors?

If the decision to standardize is made, the next question is at which stage of the development should standardization commence? If the standardization procedure is initiated too early, a standardization committee might reject a technology for being immature, which might complicate later standardization attempts. If the standardization procedure is initiated too late, major modification to existing implementations due to changes in the definition can occur.

Once the standardization timing is decided upon, the correct standardization venue must be selected. Helping to find the most appropriate venue for a new technology is the main goal of this document.

1.1 Why is standardization important?

The following is a list of the most common reasons for standardizing a networking protocol published by Stephen Byron Cooper [5].

Practice A programmer might decide to create a field in a data packet with a code field where "1" means "Accept" and "2" means "Reject". But unless this interpretation of the code is made available to other programs, that program will only be able to send messages to the same program running on a different computer. Networking protocols ensure that no one programmer has the responsibility for deciding the operating procedure for a networked function.

Competition Published standardized networking protocols enable competition. With a common standard to reference, any software house can produce programs which are automatically compatible with other programs running in the same field. This enables competition, which promotes innovation and lowers prices.

Trade Secrets Some networking standards are proprietary. A company may decide to keep its operating protocols an in-house secret to prevent other companies competing in a field that they dominate. Within the company, protocols have to be written and circulated to ensure that all their programs are compatible. This proprietary system might involve a wide range of functions and cover several different protocols.

Mixed Implementations A networked system could involve a combination of both "open" (publicly available) and "closed" (proprietary secrets) protocols. A new application may require a standard protocol to be adapted in order to function correctly. In this instance, the company creating the software is not following existing protocols, but creating a new one.

Innovation Some situations require a company to create its own new protocol in order to release a new product to the public. International standards bodies do not produce new standards quickly, so an innovative company may have to produce new standards and publish them themselves, hoping that other companies will adopt the standard and create extra facilities for the new product. This scenario is particularly seen in the fast developing field of wireless networks. There are many open standards in this area which were originally created by a company rather than a standards body. Many are later adopted as an international standards.

Associations A number of trade groupings create user groups to support a specific area of implementation – such as industrial applications or process flow networking for utility companies. This enables a group of producers to promote their products within a framework of mutual support among their users. Other trade associations are created by the holders of patented protocols to generate income from the patent by encouraging other companies to pay a fee to use them and expand the protocol's popularity.

1.2 When should I standardize?

Determining the appropriate point in time for standardization can be tricky as one needs to find a good balance between readiness of the technology and readiness of the competition. The readiness of the technology is how far the technology is developed already and how high the acceptance ratio by the desired communities is. The competition depends on the topology of the market and is the adoption probability of any competing technology, which if it was accepted, would make the acceptance of our technology impossible. We show this behavior using a simple example. Figure 1 shows a possible timeline for the adoption probability of some new technology. The dashed red line is the probability that the standardization committee would adopt the technology at this point in time. This depends on the maturity of the technology and the readiness of the standardization committee members to accept such a technology. The dotted blue line is the probability that a competitor standardized a similar technology such that our technology is not needed anymore. The solid green line is the adoption probability including the risk of a competitor adopting his technology before. We assume for the sake of simplicity that the adoption probabilities of the technologies are linearly increasing and decreasing independent of each other and thus we can simply multiply the probabilities to get the

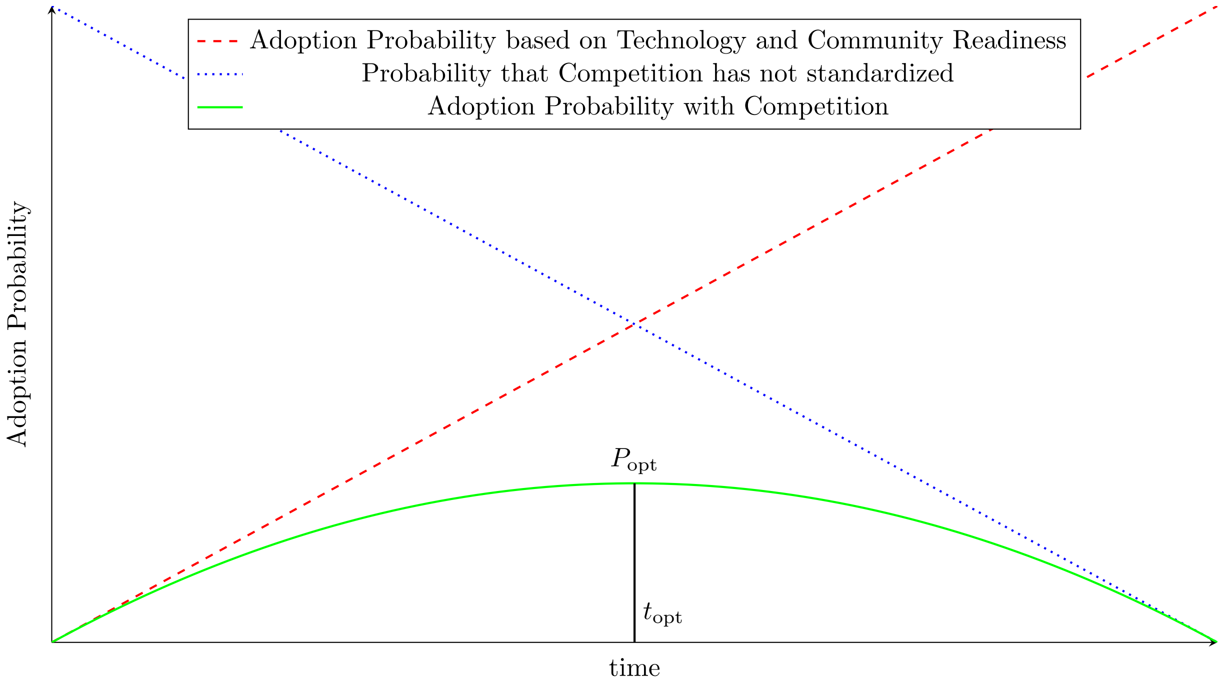

Figure 1: Example of an adoption probability for a standard over time.

actual adoption probability over time for our technology. We can see that the optimal time to attempt standardization in this example is at time t_{opt} with probability P_{opt}. Finding t_{opt} is difficult since it depends on the standardization venue's philosophy, the members of the responsible groups within the standardization venue, and the behavior of any competitors. In order to get a feeling for a standardization venue it is important to know which people to contact for a certain topic.

1.3 Where should I standardize?

Figure 2 shows a possible selection process for deciding which standardization venue is suitable for a technology[1]. Some standardization venues have overlapping standardization areas, such as the IETF and the W3C Consortium which both standardize application layer protocols. In such a case both venues should be looked at to find the most suitable venue.

IETF The Internet Engineering Task Force (IETF) is a large international community that produces technical documents for technologies applicable to the Internet. There are many widely used IETF standards for different network layers. Some famous standards are ARP [6] and PPP [7] in the data link layer, IPv4 [8], DHCP [9], and ICMP [10] in the network layer, UDP [11] and TCP [12] in the transport layer, and DNS [13, 14], FTP [15], HTTP [16], NFS [17], SMTP [18, 19], and TLS [20, 21] in the application layer. The IETF community is separated into the engineering part (IETF) which works on concrete proposals for standards and the Internet Research Task Force (IRTF) which looks at experimental topics that are not yet ready for standardization.

W3C The World Wide Web Consortium (W3C) does not produce standards by itself, but publishes recommendations which are typically treated as Web standards. Famous W3C recommendations include HTML [22], PNG [23], and CSS [24].

[1] This flowchart should only be used to get a rough idea about the different areas and might not be correct or complete.

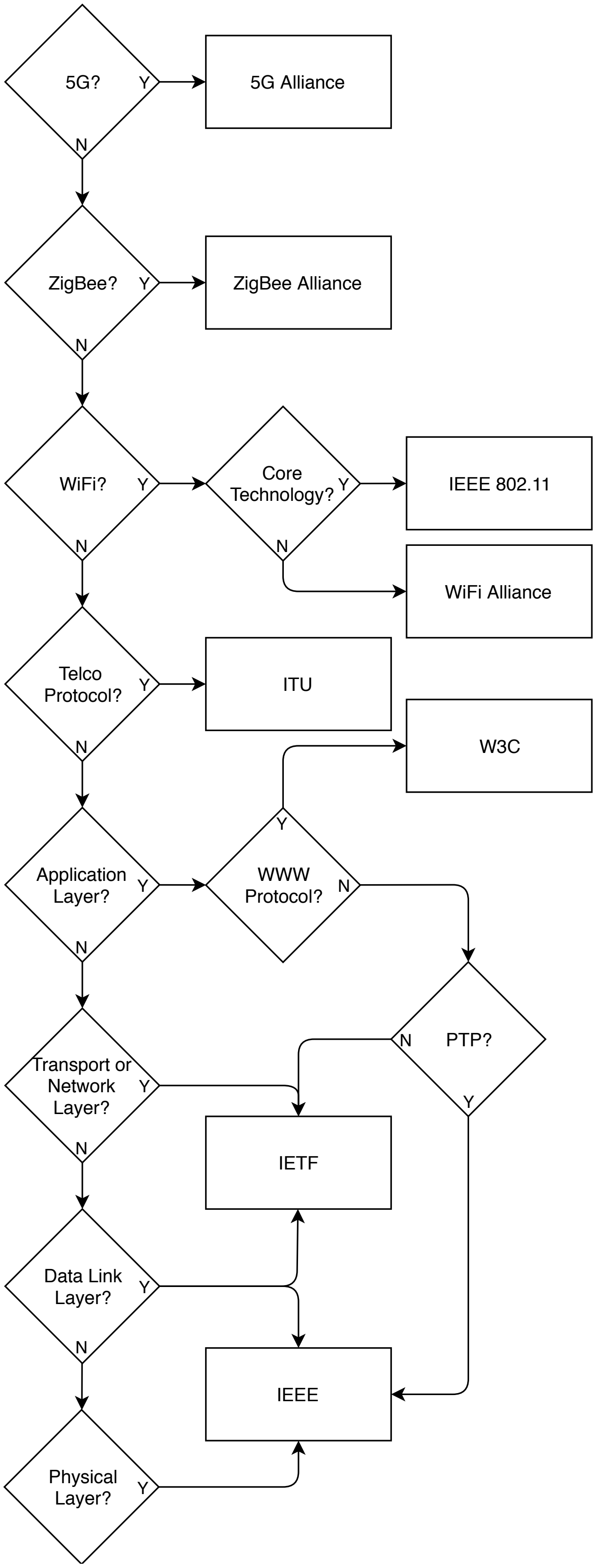

Figure 2: Flowchart for standardization venue selection

IEEE The IEEE venue focuses on standards for physical and data link layer protocols. Their standards include commonly used link layer protocols such as Ethernet (802.3) [25] and WiFi (802.11) [26] but also some application layer protocols such as PTP [27].

WiFi Alliance The WiFi Alliance standardizes IEEE 802.11 related technologies such as Wi-Fi Protected Access (WPA).

Zigbee Alliance The Zigbee Alliance produces standards for the Zigbee protocol, a low power wireless communication protocol. Zigbee is based on the IEEE 802.15.4 standard for low-rate wireless networks [28] in a similar way as WiFi Alliance is based on IEEE 802.11. Standards include the Zigbee protocol itself [29], Dotdot [30] which is an open standard for communication between IoT devices, and Smart Energy which is a protocol to manage energy-related devices.

ITU The International Telecommunication Union (ITU) standardizes technologies mostly related to encodings such as ASN.1 [31], X.509 certificates [32], but also communication protocols such as ISDN and DSL.

5G Alliance 3rd Generation Partnership Project (3GPP) combines the effort of telecommunication standardization committees of different regions, such as ETSI [33] for Europe or ATIS [34] for the US. 3GPP standardized core telecommunication technologies such as 3G [35] and 4G [36].

ETSI The European Telecommunications Standards Institute (ETSI) is responsible for European standardization in the area of telecommunication.

1.4 How does the standardization process works?

The process of getting a technology standardized depends on the venue. This Section roughly describes how the standardization process works and provides references for more detailed information for each venue.

IETF A document that should become a standard starts as an Internet-Draft submitted by an individual or a set of individuals. A suitable working group can then adopt the Internet-Draft to work together on improving the Internet-Draft as a whole. The Internet-Draft can be submitted to the RFC editor by an independent individual or a working group. [37] As soon as the RFC is published, it can enter the standards track as a "proposed standard", turn into a "draft standard" and finally become a full "Standard". [38]

There is an explicit track for research topics in the IETF called Internet Research Task Force (IRTF), which usually does not deal with specific proposals but handles long-term exploration of a research area. Depending on the project, it makes more sense to join an IRTF group, but typically IRTF groups do not produce standards.

W3C The W3C is split into working groups that cover similar topics or technologies such as HTML, SVG, or Internationalization. In order to join a working group, you need to first become a member of W3C which comes with an annual fee depending on the organization's revenue. W3C holds annual technical plenary meetings to have face-to-face discussions on relevant working group topics. The W3C Process Document [39] describes how standards (W3C recommendations) are usually created. The process can be roughly described in four steps: (1) generate interest in a relevant topic, (2) write proposal for new working groups on this topic, (3) group members collaborate with invited experts to create specifications or guidelines, (4) the advisory committee reviews the document and if there is support publishes it as a W3C recommendation.

IEEE Standardization in the IEEE is driven by the IEEE Standards Association (IEEE SA). The standardization process of the IEEE can be separated into 6 steps as shown in Fig. 3:

1. **Initiating the Project:** People who have an idea for a new project form a study group and write a Project Authorization Request (PAR) that within 6 months has to be accepted by several committees. Acceptance of the PAR marks the official beginning of the project.

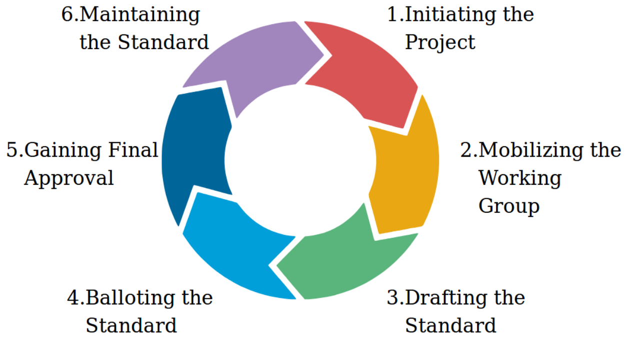

Figure 3: IEEE Standards Process as described in [40]

2. **Mobilizing the Working Group:** A working group for a project is open to individuals for individual standards projects or representatives with an IEEE SA Corporate membership for corporate standards projects.
3. **Drafting the Standard:** The working group writes the standard document.
4. **Balloting the Standard:** After the standard document has been written, the Standards Committee forms a ballot group of interested individuals and entities. After one or two months of collecting votes, if a specific number of voters agree on adapting the document, the document enters the final stage of approval.
5. **Gaining Final Approval:** After passing the ballot vote, the IEEE SA Standards Board decides whether to accept or reject the standard.
6. **Maintaining the Standard:** Adjusting standards is done by issuing a corrigenda for technical or semantic errors or errata sheet for typographical and editorial issues. Corrigendas require a new PAR while errata sheets do not.

WiFi Alliance The WiFi Alliance is a relatively closed community and participation requires a membership with an annual fee.

Zigbee Alliance In order to become a member of the Zigbee Alliance and influence the certification and standardization process, an annual fee has to be paid. There are different types of members (promoter, participant, and adopter) with different fees and the member's possibilities (e.g., participate in working groups or attend meetings) depend on the membership type. In addition, producing commercial products using Zigbee is only allowed for Zigbee Alliance members.

ITU The ITU is separated into study groups for different topics that are assigned specific questions and recommendations (standards). A study group works on answering their assigned questions and prepares draft recommendations which then have to be approved by the World Telecommunication Standardization Assembly (WTSA).

5G Alliance The 3GPP 5G Alliance is organized hierarchically with three specification groups (Radio Access Networks, Service & System Aspects, or Core Network & Terminals) consisting of several working groups (e.g., Security, Architecture, or Codec). The Project Co-ordination Group (PCG) oversees the work of the specification and working groups.

2 Privacy and Trust Enhancing Technologies related Information

2.1 IETF

The IETF's stance on privacy aspects of technologies they standardize has changed over the years. Around twenty years ago, after being requested to add capabilities for wiretapping into a media gateway protocol, the IETF decided to refuse the request and released RFC 2804 [41] stating that: "The IETF has decided not to consider requirements for wiretapping as part of the process for creating and maintaining IETF standards." After the Snowden's disclosure of mass surveillance by the NSA in 2013, the IETF took an even stronger stance for privacy in RFC 7258 [42] stating that: "Pervasive monitoring is a technical attack that should be mitigated in the design of IETF protocols, where possible." There is an interesting article in the Internet Protocol Journal [43] discussing this privacy history in the IETF and current challenges related to DNS privacy. There are a few IETF groups related to privacy that might be relevant for PET projects, and here we mention a few relevant projects in these groups.

Privacy Enhancements and Assessments Proposed Research Group mainly focuses on privacy of data collection and handling of existing databases. The following privacy related talks were given during IETF104 in this group: A talk about cryptographic access control and decentralized directory service (reclaimID). Another talk was about core principles of data collection (Tor Metrics), which are data minimalisation, source aggregation, and transparency. Two talks were about differential privacy, which is an interesting approach to privacy. "Data Privacy in Application Logs", which looks at different techniques for anonymizing personal data: Deletion, Masking, Aggregation, Generalization, Categorization, Tokenization, Differential Privacy, and Encryption (access control). "Differential Privacy" gives a quick overview of differential privacy, see RFC 6973 "Privacy Considerations for Internet Protocols".

TLS Working Group is maintaining existing, and developing new versions of TLS, and has recently published the standard for TLS 1.3. The Server Name Indication (SNI) in TLS is a good example of the difficulty of achieving certain privacy properties in the Internet. It shows that it might not be possible to achieve a complex goal, such as privacy, by modifying a single protocol.

The SNI is sent during the TLS handshake, in the client handshake message, to indicate which service to connect to at the destination IP address. Any on-path observer can read the SNI since it is sent in the cleartext part of the client handshake message and know which service the client connects to. The client has to send the client handshake message in cleartext, and the SNI has to be sent in the client handshake message to indicate which service to connect to. A possible solution is that the server, which forwards incoming requests to the services specified in the SNI, adds a DNS resource record with a public key used to encrypt the SNI. A client retrieves this public key, and uses it to encrypt the SNI, generating an encrypted SNI (ESNI) which is then added to the client handshake. The issue seems to be solved, but an attacker can still trivially link DNS requests and responses, which are cleartext, before a connection was established with the established TLS session. A possible mechanism to retrieve DNS queries, which does not leak DNS requests and responses, is to create a persistent encrypted session with the DNS service, for example using DNS over HTTPS (DoH), or DNS over TLS (DoT).

2.2 W3C

There is a W3C working group responsible for privacy in Web recommendations.

Privacy Interest Group, which is part of the "Privacy Activity", tries to improve the support for privacy in the World Wide Web. This interest group discusses privacy issues for Web recommendations of other working groups, and their document is a good starting point to check for privacy issues in projects that want to be standardized. [2]

References

[1] Network Security Group of ETH Zürich. *Network Security Group of ETH Zürich*. 2020. URL: `https://netsec.ethz.ch` (visited on 06/14/2020).

[2] Draft of their privacy guidance document: https://w3c.github.io/privacy-considerations

[2] NGI Initiative. *Next Generation Internet (NGI)*. 2020. URL: https://www.ngi.eu/ (visited on 06/14/2020).

[3] NLnet foundation. *Privacy & Trust Enhancing Technologies*. 2020. URL: https://nlnet.nl/PET/ (visited on 06/14/2020).

[4] European Telecommunications Standards Institute (ETSI). *Why standards*. 2019. URL: https://www.etsi.org/standards/why-standards (visited on 07/31/2019).

[5] Stephen Byron Cooper. *What Are the Advantages of Standardized Networking Protocols?* 2019. URL: https://itstillworks.com/advantages-standardized-networking-protocols-7475623.html (visited on 07/31/2019).

[6] D. Plummer. *An Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware*. RFC 826. IETF, Nov. 1982. URL: http://tools.ietf.org/rfc/rfc0826.txt.

[7] W. Simpson. *The Point-to-Point Protocol (PPP)*. RFC 1661. IETF, July 1994. URL: http://tools.ietf.org/rfc/rfc1661.txt.

[8] J. Postel. *Internet Protocol*. RFC 791. IETF, Sept. 1981. URL: http://tools.ietf.org/rfc/rfc0791.txt.

[9] R. Droms. *Dynamic Host Configuration Protocol*. RFC 2131. IETF, Mar. 1997. URL: http://tools.ietf.org/rfc/rfc2131.txt.

[10] J. Postel. *Internet Control Message Protocol*. RFC 792. IETF, Sept. 1981. URL: http://tools.ietf.org/rfc/rfc0792.txt.

[11] J. Postel. *User Datagram Protocol*. RFC 768. IETF, Aug. 1980. URL: http://tools.ietf.org/rfc/rfc0768.txt.

[12] J. Postel. *Transmission Control Protocol*. RFC 793. IETF, Sept. 1981. URL: http://tools.ietf.org/rfc/rfc0793.txt.

[13] P.V. Mockapetris. *Domain names - concepts and facilities*. RFC 1034. IETF, Nov. 1987. URL: http://tools.ietf.org/rfc/rfc1034.txt.

[14] P.V. Mockapetris. *Domain names - implementation and specification*. RFC 1035. IETF, Nov. 1987. URL: http://tools.ietf.org/rfc/rfc1035.txt.

[15] J. Postel and J. Reynolds. *File Transfer Protocol*. RFC 959. IETF, Oct. 1985. URL: http://tools.ietf.org/rfc/rfc0959.txt.

[16] M. Belshe, R. Peon, and M. Thomson. *Hypertext Transfer Protocol Version 2 (HTTP/2)*. RFC 7540. IETF, May 2015. URL: http://tools.ietf.org/rfc/rfc7540.txt.

[17] Sun Microsystems. *XDR: External Data Representation standard*. RFC 1014. IETF, June 1987. URL: http://tools.ietf.org/rfc/rfc1014.txt.

[18] J. Postel. *Simple Mail Transfer Protocol*. RFC 821. IETF, Aug. 1982. URL: http://tools.ietf.org/rfc/rfc0821.txt.

[19] D. Crocker. *STANDARD FOR THE FORMAT OF ARPA INTERNET TEXT MESSAGES*. RFC 822. IETF, Aug. 1982. URL: http://tools.ietf.org/rfc/rfc0822.txt.

[20] T. Dierks and E. Rescorla. *The Transport Layer Security (TLS) Protocol Version 1.2*. RFC 5246. IETF, Aug. 2008. URL: http://tools.ietf.org/rfc/rfc5246.txt.

[21] E. Rescorla. *The Transport Layer Security (TLS) Protocol Version 1.3*. RFC 8446. IETF, Aug. 2018. URL: http://tools.ietf.org/rfc/rfc8446.txt.

[22] Arron Eicholz et al. *HTML 5.2*. W3C Recommendation. https://www.w3.org/TR/2017/REC-html52-20171214/. W3C, Dec. 2017.

[23] David Duce. *Portable Network Graphics (PNG) Specification (Second Edition)*. W3C Recommendation. http://www.w3.org/TR/2003/REC-PNG-20031110/. W3C, Nov. 2003.

[24] Ian Hickson et al. *Cascading Style Sheets Level 2 Revision 1 (CSS 2.1) Specification*. W3C Recommendation. http://www.w3.org/TR/2011/REC-CSS2-20110607/. W3C, June 2011.

[25] "IEEE Standard for Ethernet". In: *IEEE Std 802.3-2018 (Revision of IEEE Std 802.3-2015)* (Aug. 2018), pp. 1–5600. DOI: 10.1109/IEEESTD.2018.8457469.

[26] "IEEE Standard for Information technology-Telecommunications and information exchange between systems Local and metropolitan area networks-Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications". In: *IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012)* (Dec. 2016), pp. 1–3534. DOI: 10.1109/IEEESTD.2016.7786995.

[27] "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems". In: *IEEE Std 1588-2008 (Revision of IEEE Std 1588-2002)* (July 2008), pp. 1–300. DOI: 10.1109/IEEESTD.2008.4579760.

[28] "IEEE Standard for Low-Rate Wireless Networks". In: *IEEE Std 802.15.4-2015 (Revision of IEEE Std 802.15.4-2011)* (Apr. 2016), pp. 1–709. ISSN: null. DOI: 10.1109/IEEESTD.2016.7460875.

[29] Zigbee Alliance. *Zigbee 3.0*. 2019. URL: https://zigbee.org/zigbee-for-developers/zigbee-3-0/ (visited on 11/21/2019).

[30] Zigbee Alliance. *Dotdot*. 2019. URL: https://zigbee.org/zigbee-for-developers/dotdot/ (visited on 11/21/2019).

[31] ITU-T. *Abstract Syntax Notation One (ASN.1): Specification of basic notation*. Recommendation X.680. Geneva: International Telecommunication Union, Aug. 2015.

[32] ITU-T. *Public-key and attribute certificate frameworks*. Recommendation X.509. Geneva: International Telecommunication Union, Sept. 2016.

[33] European Telecommunications Standards Institute (ETSI). *ETSI homepage*. 2019. URL: https://www.etsi.org (visited on 11/22/2019).

[34] Alliance for Telecommunications Industry Solutions (ATIS). *ATIS homepage*. 2019. URL: https://www.atis.org (visited on 11/22/2019).

[35] European Telecommunications Standards Institute (ETSI). *3th Generation (UMTS)*. 2019. URL: https://www.etsi.org/technologies/mobile/3g (visited on 11/25/2019).

[36] European Telecommunications Standards Institute (ETSI). *4th Generation (LTE)*. 2019. URL: https://www.etsi.org/technologies/mobile/4g (visited on 11/25/2019).

[37] IETF. *Independent Submissions*. 2019. URL: https://www.rfc-editor.org/about/independent (visited on 07/31/2019).

[38] S. Bradner. *The Internet Standards Process – Revision 3*. RFC 2026. IETF, Oct. 1996. URL: http://tools.ietf.org/rfc/rfc2026.txt.

[39] Coralie Mercier. *Tips for Getting to Recommendation Faster*. 2015. URL: https://www.w3.org/2019/Process-20190301/.

[40] IEEE. *IEEE Standards Development Lifecycle*. 2019. URL: https://standards.ieee.org/develop/index.html (visited on 11/22/2019).

[41] IAB and IESG. *IETF Policy on Wiretapping*. RFC 2804. IETF, May 2000. URL: http://tools.ietf.org/rfc/rfc2804.txt.

[42] S. Farrell and H. Tschofenig. *Pervasive Monitoring Is an Attack*. RFC 7258. IETF, May 2014. URL: http://tools.ietf.org/rfc/rfc7258.txt.

[43] Geoff Huston. "DNS Privacy and the IETF". In: *The Internet Protocol Journal* 22.2 (July 2019), pp. 2–13. URL: http://ipj.dreamhosters.com/wp-content/uploads/2019/07/ipj222.pdf.