GFCE Global Good Practices

Internet Infrastructure Initiative (III)

GFCE
Global Forum on Cyber Expertise

Preface

The economic growth and social benefits that were boosted by the internet require a sustained trust in the cyber domain. This level of trust is being threatened by cyber-attacks (e.g. hacking), cybercrime (e.g. ransomware) and unwanted messages (e.g. spam). The global exposure of these threats requires a collaborative response to build capabilities that improve internet security.

A foundation for internet security is provided by the ecosystem of protocols, standards, technology, practices and organisations that are the internet's infrastructure. An important contribution to a secure and resilient internet infrastructure is the adoption and deployment of open, security-oriented internet standards. Initiatives to promote the use of these standards, such as the World IPv6 launch day and DNSSEC adoption campaigns, have been initiated and supported by organisations around the world. More wide-spread collaboration and extension of these initiatives are required to reap the benefits of a secure internet. An Internet Infrastructure Initiative (III) should be established, in order to bring stakeholders together, raise awareness and provide support for standards deployment. This initiative consists among others out of a cooperation and a website to raise awareness and to test standards-compliance.

This Global Good Practice on Internet Infrastructure helps policy-makers and political leaders in defining sustainable and efficient efforts to stimulate adoption of open internet standards. This document provides a set of good practices to develop an effective national internet infrastructure deployment program, that is aligned in the international Internet Infrastructure Initiative.

1. Introduction

Internet infrastructure & internet standards

Internet infrastructure is the ecosystem of protocols, standards, technology, practices and organisations that keep the internet running. An open, stable and secure internet infrastructure is key to sustaining the economic growth and social benefits that were boosted by the internet. These internet-driven innovations require the continuation and improvement of trust in the cyber domain that is threatened by cyber-attacks (like Distributed Denial-of-Service attacks), cybercrime (hacking, malware, phishing, botnets) and unwanted messages (like (e-mail) spam). The global exposure of these threats requires a collaborative, global response to secure the internet infrastructure to sustain the benefits of the internet.

An important contribution to a secure and resilient internet infrastructure is the adoption and deployment of security-related internet standards. An Internet standard is a specification that has been approved by the Internet Engineering Task Force (IETF). An Internet Standard is characterised by a high degree of technical maturity and by a generally held belief that the specified protocol or service provides significant benefits to the Internet community. The adoption of these standards helps to promote a consistent, universal and secure use of the internet worldwide.

Internet infrastructure initiative

The adoption of security-related and other key internet standards requires continuous investments by key stakeholders, including government, industry, civil society and the technical community. An infrastructure initiative should be established by governments. The Internet Infrastructure initiative aims to bring stakeholders together, to raise awareness and provide support to all stakeholders with the deployment of internet standards and related technologies. This document contains good practices for achieving these objectives.

The internet infrastructure initiative (III) promotes the use of the following internet standards:

- **IPv6**: a major extension of the internet address range and enabler of security capabilities
- **DNSSEC**: security extensions for the internet domain name infrastructure
- **TLS, HTTPS, DANE and STARTTLS**: secured connections between internet users and services
- **DKIM, SPF and DMARC**: anti-phishing and anti-spoofing measures

In a next phase, the initiative can be expanded with activities aiming at building or improving the key elements that enable a properly functioning internet in each country, such as neutral IXPs (Internet Exchange Points), running a national domain registry (ccTLD), development of open source software, and routing security (MANRS, (ISOC, 2014-2016)). Furthermore, during the ICANN55 meeting in 2016, ICANN unveiled the Identifier Technology Health Indicators initiative (ICANN, 2017), with the goal to measure the health of the Internet's identifier system. These activities are complementary, but are not part of the scope of this document.

Goal and outline of this document

This document describes the good practices which can be part of an internet infrastructure initiative. The target audience comprises public policy-makers, who can use these good practices to develop a (national) policy or strategy for developing III programs. The content of this document is prepared for policy-makers that have basic knowledge of the internet infrastructure, but are no expert in the field.

In the next chapter, a high-level overview on the internet standards that are in the current scope of the initiative is given. Chapter 3 presents the III's set of good practices. Chapter 4 contains more background information on the standards, including a high-level description of the technical workings, the benefits that they provide, the current global adoption rates, and the challenges which need to be overcome when promoting these standards.

2. Background internet standards

This chapter provides an overview of the security-related internet standards that are promoted through the III that are in the scope of this document. These open internet standards are developed by the internet industry and are published by the Internet Engineering Task Force (IETF, 2017). For a more elaborate description of these standards, including benefits, challenges and adoption status, see chapter 4.

The relationship between the selected internet standards that are part of the III is shown in figure 1.

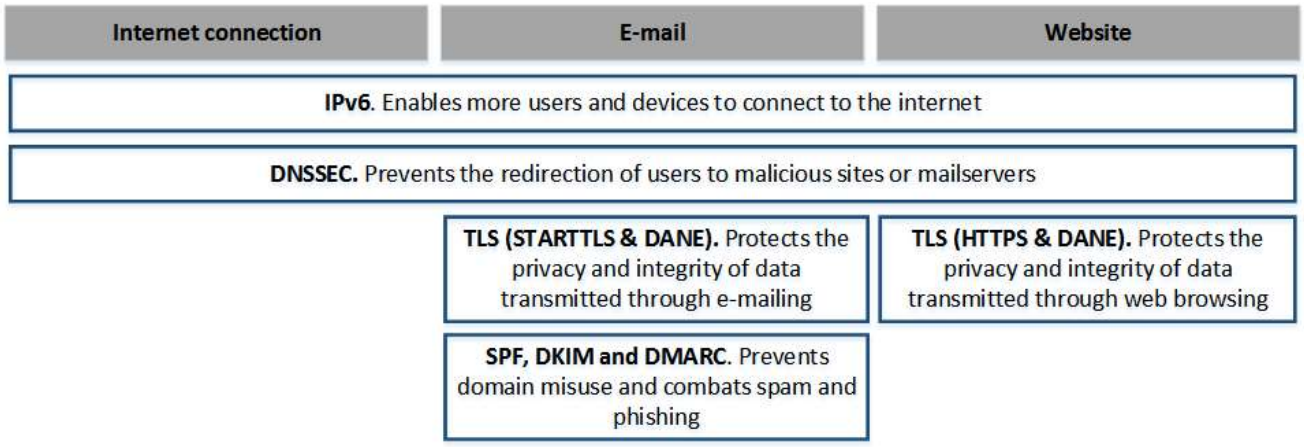

Figure 1: an overview of the internet standards part of the scope of this document

TLS & HTTPS. *Protects the privacy and integrity of transmitted data*

The Transport Level Security protocol (TLS) provides protection of all data transmitted between two end-points (user and service) on the internet by encrypting the data stream. TLS has a wide array of applications, including securing of website interaction and the transport of e-mail. The most common use of TLS is creating a secure transport mechanism for web browsing (TLS is used by the higher-level HTTPS protocol). A secured website can be identified by a “lock” symbol in the address bar, as well as by a URL that begins with "https://" rather than "http://". The underlying use of TLS provides basic assurance that the transmitted information is not being read or forged by malicious actors and that a user is communicating with precisely the website or service that he/she intends to communicate with (as opposed to a malicious copy). Because websites nowadays process lots of sensitive data, such as payment transactions and personal information, the importance of TLS to our privacy and security can therefore not be overstated. Two related protocols are DNS-based Authentication of Named Entities

(DANE) and STARTTLS. DANE is an additional security mechanism, enhancing the effectiveness of TLS. STARTTLS is used to enforce the use of TLS in existing technologies, such as e-mail transport.

DNSSEC. *Prevents the redirection of internet users to malicious sites or mail servers.*
When a user visits a certain web address such as www.thegfce.com, the browser needs to retrieve the corresponding IP-address to access the website. It is important that the IP-address information is correct. If hackers manipulate that address information, users can be redirected to a hacker's website or tempted to send or retrieve e-mails from a mail server that is controlled by the hacker. The Domain Name System Security Extensions (DNSSEC) ensures that the user retrieves the correct IP-address of the website or service. DNSSEC is *not* only for the web, but also for any other internet services, such as e-mail, instant messaging and voice-over-IP. Moreover, DNSSEC is used as a building block to provide authenticity and integrity for other protocols such as DANE.

SPF, DKIM & **DMARC**. *Prevents domain misuse and combat spam and phishing.*
The current e-mail system cannot prevent malicious actors sending e-mails on behalf of legitimate organisations. The e-mail address shown in the 'From' -field can be changed ('spoofed') without any technical knowledge. The e-mail can therefore look like an e-mail that is send by 'info@organisation.com', while in fact it is sent by 'hacker@abadguy.com'. Without additional security measures, there is no way to guarantee whether an e-mail was really sent from the shown e-mail address. This makes it difficult for an organisation to detect and filter phishing mail. A way to prevent e-mail spoofing is by validating the identity of the originator or the originating e-mail server. This is called e-mail authentication. SPF, DKIM and DMARC are techniques providing the means for this type of authentication.

IPv6. *Enables more users and devices to connect to the internet and provides security capabilities.*
Every device on the internet needs a unique identifier, a kind of address, to communicate with other devices. This is called the IP-address. Currently, IPv4 is the most used version of the Internet Protocol (IP) and facilitates 4.3 billion IP-addresses. Nearly all of these addresses are already assigned. IPv6 facilitates trillions of addresses, and is therefore necessary to scale up the internet and connect more uses and devices. It also solves several security issues and technical limitations, making the internet more robust, efficient and secure.

3. Good practices

This chapter presents the set of these good practices that provide guidance for deploying activities that contribute to achieve the objectives of the III.

Good practice 1: Establish a national multi-stakeholder cooperation to promote the security-related internet standards

A voluntary-based cooperation, which has a common goal and shared responsibility, can contribute to an increased level of internet security. Such a cooperation comprising various types of stakeholders encourages raising mutual awareness about the weaknesses in systems, discussing main challenges and solutions, and providing mutual support in taking preventive measures. This mechanism is transparent, triggers improvement, and its results are an incentive for organisations to increase efforts.

The cooperation contributes to the development of an enabling environment at the national level by raising the awareness for the need to implement available internet standards. It also contributes to partnership building by creating mechanisms and frameworks for cooperation and collaborative learning. It therefore develops capacities of the participating stakeholders through cooperation, awareness raising, focused workshops and discussions, expert support and advice, exchange of resources, and development of guidelines for the deployment of the security-related and other key internet standards.

Actors (for who is this good practice document?)

The implementation of security standards is a collective effort by many organisations. The cooperation stimulates multi-stakeholder cooperation and sharing expertise.

A typical cooperation is comprised of technical Internet-related organisations and departments - the national Computer Security Incident Response Team (CSIRT), the Ministry or National Regulatory Authority in charge of Internet policymaking, civil society (ISOC), the technical community (RIRs, ICANN) and umbrella organisations representing businesses in the ICT-sector: e.g. Internet Service Providers (ISPs), ICT solution providers, manufacturers, and hosting providers. There can also be other organisations that underpin and support the activities as long as their participation is not used to promote their own products or services.

What is the timeline for implementation?

The local environment and context highly influences the time scale for establishing such a cooperation. No general scheme exists, but experiences by other established cooperations may be of help. Drawing from practice in the Netherlands, it took about one year to set up an operational cooperation.

Once established, the lifetime of a cooperation depends on the initial goal; e.g. the cooperation could dissolve when a certain percentage of implementation has been achieved. In principle, the cooperation continues to be useful as long as implementation of the selected set of internet standards does not achieve a certain maturity. For certain standards this can take a long time. For instance, a similar Task Force for the promotion of IPv6 in the Netherlands still exists after about ten years, because of the slow pace of IPv6 adoption.

How can this be implemented?

Practical steps for implementation: principles & recommendations:

- Involve organisations and institutions particularly interested in improving the level of trust through the use of security related internet standards. Participation should have a low barrier - open to all stakeholders that support the mission and activities, and which will not use the cooperation for product promotion, marketing and direct sales.
- Prepare and agree a code of conduct and act on accordingly on a set of basic principles for participation.
- Find the most meaningful and feasible way of participation for each organisation. Organisations should contribute to the cooperation by allowing their employees to be involved in activities, such as hosting or facilitating meetings, or utilising their communication channels for outreach.
- Organise the cooperation in a lightweight 'organised network' rather than an organisation, with no headquarters, employees or formal partnerships.
- Avoid unnecessary overhead costs and bureaucracy. Ensure a basic budget - through contributions of several stakeholders and possibly the government - for basic support (active chairperson, website and tools development, and secretariat functions). Other contributions should be in-kind by partners.
- Focus the discussions and work on technology - challenges and solutions - rather than on broad aspects.

What are the challenges?

The following challenges can be identified:

- Different national approaches that need to be examined. In general, this cooperation works best in an environment that is already acquainted with multi-stakeholder initiatives. In environments that are not susceptible to a multi-stakeholder model, a different approach might be considered.
- The biggest challenge is in the initiating phase. Most organisations in the private sector acknowledge the need for action, but are not willing or do not feel the responsibility of taking the necessary first step.
- A possible extension of the cooperation beyond national borders would increase the number of requests for support, which conflicts with the voluntary, low-cost support activity of the cooperation. It is therefore better if the cooperation activities are adapted by different countries to make it locally-specific.

Example

Many cooperations with the task to promote internet standards already exist. Japan has established a promotion body to increase IPv6 adoption (IPv6 Promotion Council, 2002). Government agencies are responsible for the grand design, strategic planning and budgets. The industry and private companies develop R&D and trial projects. For the general public, the body writes press releases, organizes events and performs road shows. A consumer monitoring group provides feedback on products.

Many countries, including the EU (Ministry of Science, ICT & Future Planning South Korea, 2014) and Saudi Arabia (Al-Furaih, 2014) have similar Task Forces. For more examples of IPv6 task forces, see the document of the Internet Governance Forum (Chalmers & Degezelle, 2015).

In the Netherlands, the “Platform for internet standards” promotes, amongst others, security-related internet standards:

- The Dutch government embraced the public interest of this initiative and became an active driving force to set up this cooperation. It gave initial funding (being a majority financial contributor) and gathered interests and participation. After two years, the Dutch government’s involvement in terms of money and time spent has decreased (but is still substantial) as a result of increased involvement by other (inter)national stakeholders. The cooperation focusses only on technical standards, as it mainly comprises technical organisations and departments.

- The Dutch Platform for internet standards organises two seminars or workshops a year for interested parties. The events are narrowly focused - such as on e-mail security - covering implementation practices and tools, preferably open source, and how various tools complement each other. It also published a paper on encryption and TLS that takes political aspects into account.
- Each year the number of companies and organisations that took part in the cooperation has increased. This is partially due to an increase in the use of the publicly provided testing tool (see: Good Practice 2 "Create an internet standards awareness website"). The positive competition to receive a 'badge of honour' on the testing tool webpage has improved implementation of internet security standards across the Netherlands.

Good practice 2: Create an internet standards awareness website

To stimulate awareness, enable and encourage individuals and organisations to use and deploy important internet standards, a website should be created. This website should provide information to motivate adoption and provide tools for testing compliance with these standards.

This website should be a free and public service. The visitor should find comprehensible supporting documentation about the internet standards, complemented with arguments and pitfalls regarding their deployment. Further, the visitor can - in real time - check any given domain name, whether used as a website or within an e-mail address, for standards-compliance. The test results include suggestions for taking next steps, such as the advice to contact one's Internet provider to enable IPv6. The online tool may also act as a communication channel and point of contact for any national initiative related to the implementation of the various security-related and other key internet standards.

This tool contributes to the implementation of key internet standards through a variety of mechanisms:

- It raises awareness on key internet standards and provides implementation support.
- The rating system, based on testing tool results, triggers peer pressure.
- Decision-makers can get insights into the deployment-status of internet standards within their organisation and act on it.

- The press can use it to write about organisations who lack the necessary standards. This could have political impact. For example, the Dutch minister of the Interior promised to fix the poor security of municipal e-mail systems across the country after the press addressed this issue.

While the tool provides support for the implementation of internet standards, for most organisation this would not be sufficient and a more comprehensive approach is needed. A cooperation of organisations could provide the required support and it can be used to discuss the challenges which need to be overcome when implementing the standards (see: Practice "Establish a national multi-stakeholder cooperation to promote standards").

Actors (for who is this good practice?)

Targeted stakeholders are in general all organisations that heavily rely on the internet to communicate with users. Typically, these stakeholders are ISPs (access and e-mail), government authorities (e-governance) and the business sector (e-commerce). Yet anyone, including individuals, can use the test tool to check the level of implemented security-related internet standards in their own system.

What is the timeline for implementation?

Development of a website and a testing tool can run in parallel with setting up a cooperation (see: Practice "Establish a national multi-stakeholder cooperation to promote standards"), provided there is a small group of initiators willing to invest in it.

In the case of a straightforward duplicated/translated version of existing practices (see example below), it will take a couple of months to develop. When there are specific needs and adaptations required, the development can take up a year.

After the initial development, it needs to be improved and updated on a continuous basis (new functions, user feedback, bugs etc.). The goals of the platform determine how, and how long, the tools need to be used and therefore be maintained.

How can it be implemented?

Practical steps for implementation are:

- Register a simple domain that people can remember.
- Prepare instructions in a simple non-technical language.
- Create a communication platform to promote your tool (see: Practice "Establish a national multi-stakeholder cooperation to promote standards").

- Create a support team that will answer users' questions.
- Tailor the components of the website to your national context (e.g. multiple languages).

What are the challenges?

The following challenges should be considered:

- Lack of awareness, which could be mitigated through awareness-raising campaigns (using simple terminology, potentially showcasing metrics).
- Language barriers, which may be addressed through the translation of materials and developing local content.

Example

The awareness website and testing tool made available for the GFCE Internet Infrastructure Initiative is available at www.internet.nl. It is available in English, Dutch and Polish and can be used by stakeholders in any country, for any domain and any internet connection.

Website statistics show that the testing tool is being used increasingly. The tool revealed a lack of use of key internet standards by several municipalities in the Netherlands. In response, the Minister in charge promised to increase the adoption of internet standards by all Dutch municipalities. Other institutions and communities, such as the APNIC, are moving towards implementing the awareness website.

Good practice 3: Provide economic & regulatory incentives

For most business organisations, economic incentives are a key driver. The business models for internet access, domain registration, internet certificate services, and cloud services provide multiple opportunities for economic and regulatory incentives to stimulate the adoption of internet standards. Governments should investigate the possibilities for such incentives and put these into practice. The specific set of applicable incentives should be adapted to region specific demands and circumstances.

Several types of economic incentives can be provided. For example, South Korea and Japan have provided tax reductions to companies introducing IPv6 (Ministry of Science, ICT & Future Planning South Korea, 2014), as significant investments need to be made. A certain percentage of the cost of purchasing IPv6 equipment (routers, switches) are or were tax deductible. Japan and Korea also provided logos and certifications for IPv6-enabled devices (Study Group on Advanced Use of Internet with IPv6, 2010; Howav, Hemmert, & Kim, 2010).

Another example is a subscription fee discount for DNSSEC signed domains. The two main actors involved are registrars for country codes and registries. *Registries* manage top-level domains such as .nl, while *accredited registrars* can sell the corresponding second-level domains such as internetten.nl. Many internet registries for country code top-level domains (ccTLDs) are not-for-profit organisations that are supporters of the adoption of open standards. The business interaction between these internet registries and registrars has been successfully used to stimulate open standard adoption.

For each domain subscription that a registrar sells to a customer, a fee applies that is paid to the registry. By providing a discount to the registrar for selling a DNSSEC signed domain or making a service accessible via IPv6, the registry can provide specific economic incentives to the registrar. Of course, it is the internet registry's decision to offer such a discount program, or not. Depending on the relation between the internet registry and the national government, the government may stimulate such a program.

In principle, such a campaign can temporary boost the adoption of DNSSEC and/or IPv6. It should be noted that if a campaign is discontinued at some point in time, the incentive for correctly configuring DNSSEC may get lost.

Amongst others, the internet registries AFNIC (France), EURid (Europe, .eu registry), NORID (Norway) and SIDN (The Netherlands), have launched domain registration discount campaigns for their registrars that have stimulated the adoption of DNSSEC signed domain names (DNSSEC-campaign-references). SIDN applies their "registrar scorecard" program not only to stimulate DNSSEC, but also for IPv6 promotion.

DNSSEC stimulation program implementation

For a government agency to be an effective communication partner with these registrars, the background information on the necessary implementation activities is described below.

First, a DNSSEC stimulation program requires the registry to be DNSSEC enabled in order to enable registrars to facilitate in their DNSSEC business transactions. This requires the ccTLD to be signed (which is already the case for most ccTLDs), and requires an automated domain registration system (DRS) that supports (changes to) DNSSEC registration data. Upgrading a registry's DRS to support DNSSEC registrations requires a carefully planned project that may take up to a year to execute.

Further, a registration discount program requires tools to measure the fraction of signed domain names per registrar and to calculate the periodic discounts. Such a tool should not only verify if a domain name is signed, but also if the DNSSEC data can be validated correctly. Skills for developing such tooling are similar to -but not the same as- for the internet.nl test tool (see: "Create a website for testing standards-compliance").

Practical steps for implementation are:

- The registry prepares for DNSSEC (signed ccTLD, automated DRS).
- The registry prepares registrar attributable DNSSEC and IPv6 measurements.
- The registry launches a discount campaign in collaboration with its (accredited) registrars.

Good practice 4: Lead by example

Governments can lead by example by implementing the security-related and other key internet standards in existing systems and networks and through their procurement processes.

Governments should actively promote the use of internet standards and good practices in their own infrastructure by their agencies. Governments should ensure that appropriate resources, including staff and budget, are allocated to agencies and governmental departments for implementing and configuring the standards. The requirements for security-related and other key internet standards in ICT products need to be embedded in procurement procedures and policies.

Governments need to include the adoption of internet standards in their strategic ICT-plans. Roadmaps need to be developed outlining the tactical and operational implementation activities and stakeholder responsibilities (CIO Council, 2012; MEWC Malaysia, 2008; Al-Furaih, 2014).

Many countries have already taken extensive measures to ensure government agencies lead by example. For example, US authorities have made sure that the government and public organisations pre-emptively switch to IPv6. This helps to identify and mitigate security issues and encourages the private sector to adopt IPv6 (CIO Council, 2012; Ministry of Science, ICT & Future Planning, 2014).

In the Netherlands, open internet standards are required to be included by suppliers of ICT-products and services for the government (National Cyber Security Centre, 2016). A 'comply or explain'-

mechanism is used. If a government agency procures a product that lacks the required internet standards, accountability for this needs to be reported. Similar approaches have been adopted by Sweden, the US and Spain with regards to IPv6 (Chalmers & Degezelle, 2015).

4. Comprehensive background internet standards

In this chapter, a more elaborate description is given of the security-related internet standards that are part of the current scope of the III explained in this document. This description includes the technical workings of the selected standards, the benefits they provide, the adoption challenges and the current adoption status.

What are TLS, HTTPS, DANE and STARTTLS?

The Transport Level Security protocol (TLS) provides protection of all data transmitted between two end-points (user and service) on the internet by encrypting the data stream. It has wide array of applications, including web browsing and e-mail traffic. The most common use of TLS is creating a secure environment for web browsing. HTTP is a protocol which enables the transmission of data between a webserver and a web browser. HTTPS is the secure version of HTTP and uses TLS to encrypt the transmitted data. A secured website can be identified by a lock in the (green) address bar in the user's browser and a URL that begins with "https://" rather than "http://".

HTTPS (and TLS in general) requires the use of a digital certificate, which contains information about the domain owner, the certificate issuer and the cryptographic key that is to be used for encrypted transmission. This digital certificate must be installed on the webserver by the domain owner such as a private company or government agency.

In addition to protecting the data stream between the user and a web service HTTPS and the digital certificate provides authentication of the website. HTTPS. In practice, this provides a reasonable guarantee that one is communicating with an authentic website (and not a malicious duplicate), as well as ensuring that the contents of communications between the user and web service cannot be read or forged by a hacker. Because websites nowadays process a lot of sensitive data, such as payment transactions and personal information, the importance of TLS to our privacy and security cannot be overstated (as emphasized by the Internet confidentiality statement in (Internet Architecture Board (IAB), 2014)).

Two related protocols to TLS are DANE and STARTTLS.

DANE. A shortcoming in HTTPS (TLS for web browsing) is that a user has limited means to verify that he/she is using the correct certificate (Internet Society, 2012). While he/she may see the green bar and "padlock" icon on the web browser screen, it is possible for a device in the network path between

the user and the service (such as a firewall) to terminate the encrypted connection and recreate a forged connection. This way, a user may think he/she has a secure connection, for example to his/her bank, while in reality the connection has been intercepted and is being eavesdropped on all the transmitted information. DANE ("DNS-Based Authentication of Names Entities") enables a domain owner to specify which certificate a user should use to connect to the site. For instance, a web browser supporting DANE can detect that it is not using the specified certificate, although the green bar and lock icon is visible, and notify its user. To enable the verification of authenticity and integrity of information used by the DANE protocol this information is digitally signed with DNSSEC. Next to the usage for web browsing, DANE is also gaining momentum in securing e-mail communication and instant messaging applications, such as Jabber.

STARTTLS. As described in the beginning of this chapter, TLS is used to encrypt the information exchanged between systems. Many applications already use a certain protocol, that amongst others, specifies how information is exchanged. Support for TLS can be incorporated into an existing protocol using STARTTLS. For many applications, a STARTTLS expansion has been developed, including for e-mail (SMTP protocol) and Instant Messaging (XMPP protocol).

What are the benefits?

Privacy & Confidentiality. TLS protects, amongst others, all information between client and server, e.g. when a user visits a website. This prevents malicious actors obtaining or manipulating (sensitive) data, such as payment records, personal data and confidential e-mails.

Authentication & Anti-phishing. HTTPS ensures that the visited website is legitimate and not a cloned version created by malicious actors. Phishing e-mails often send the innocent recipients to an imposter website that looks authentic. Personal information that is provided on this website, such as credit card information, is then directly sent to the hackers. Because it is difficult for criminals to receive a proper digital certificate, it is much more complicated to forge a genuine website. Because users will not be able to find the trust indicators, such as a green address bar and a lock icon, when visiting the non-authentic website, they will less likely to be misled by a phishing attack.

Increased customer trust. The web browser's trust indicators increase the level of trust a customer has in websites. Establishing trust is vital for increasing economic activity on e-commerce website (Corbitt, 2003).

Google rankings. Google has announced that having a HTTPS enabled on a website will increase the ranking position of the website in their search engine (Google, 2014).

What are the challenges to adoption?

Cost of certificates. To enable TLS on a website or a mail server, a certificate must be bought. There are also administrative cost of installation and renewing certificates prior to their expiration.

Untrusted Certificate Authorities. The number of CAs that may issue a digital certificate is relatively large. A few of these CAs have suffered a security hack (for example (Dutch Government, 2012)), which enabled their attackers to issue rogue certificates. This has undermined the trust in CAs and the mechanism to create, distribute and validate digital certificates (referred to as a public key infrastructure - PKI). The DANE protocol enables improvement of trust in the PKI (Verisign Labs, 2012).

Technical drawbacks. HTTPS can slow a website down (additional latency, caching difficulties and additional certificate revocation checks). However, when using proper configurations, the difference with the use of the insecure http protocol will be minor. With the introduction of the DANE protocol such a 'slow-down' becomes unnoticeable to the users.

What is the current adoption status?

A recent scientific publication (Felt, Barnes, King, Palrmer, & Tabriz, 2017), provides statistics on the adoption of TLS for web browsing (HTTPS). The growth in HTTPS-adoption is enormous and can be viewed from three perspectives:

- **Top websites.** Default HTTPS support among the Google Top-100 nearly doubled in 2016.
- **Network traffic.** HTTPS traffic doubled as a percentage of all web traffic from 2014 to 2017.
- **End user perspective.** A majority of desktop browsing now uses HTTPS. HTTPS usage on Android is growing and will soon replace HTTP.

There are not many statistics available on the adoption of DANE. In a recent scan of DNSSEC signed domains (because DANE depends on DNSSEC) it appears that data used by the DANE protocol is only available on 0.8% of .com domains and 1.3% of .net domains. For Alexa 100k this percentage is 4.2% (York, State of DNSSEC Deployment, 2016).

The most common application of STARTTLS is for securing e-mail traffic as part of the Simple Mail Transfer Protocol (SMTP). For encrypted messages, both sides (receiver and sender) need to deploy TLS. In 2014, Facebook reported that 95% of their notification e-mails are successfully encrypted (Facebook, 2014). Recent data from Google shows that 90% of their e-mail is encrypted (Google, 2017). This implies that many e-mail providers have already adopted STARTTLS.

What is DNSSEC?

The Domain Name System (DNS) can be regarded as the dictionary of the internet: it converts domain names into IP-addresses. For example, when a user wants to visit a certain domain, such as www.thegfce.com, the browser needs to know the corresponding IP-address to retrieve a certain web page of the website. DNS is responsible for this conversion and will, in case of www.thegfce.com, return the IPv6-address 2a00:d00:3:4::80 or the IPv4-address 178.22.85.65.

It is important that the information provided by the DNS is correct. If hackers manipulate this information, users can be redirected to a hacker's website or tempted to send or retrieve e-mails from a mail server that is controlled by the hacker. DNS Security Extensions (DNSSEC) provides a way to authenticate the DNS-information using digital signatures. This enables the user to verify that he/she is communicating with the correct internet service. DNSSEC is *not* only for accessing web pages, but also for any other internet service or protocol, such as e-mail (SMTP), instant messaging and voice-over-IP. DNSSEC operation consists of two main tasks:

- Signing: a domain name is 'signed' with a digital signature. This is done by the organisation managing the system (called a name server) that publishes the DNS data for a domain such as www.thegfce.com. This could be the owning organisation of the domain name itself, or the organisation could hire an external registrar or web-hosting provider to include digital signature data on their behalf.
- Validating: the digital signature is verified when the DNS data is retrieved, to ensure the data was not modified in transit. In most cases, the ISPs provide the DNS-services for end-users and are therefore an important stakeholder for the validation-side of DNSSEC. If an ISP does not provide this service, users do have options to perform DNSSEC validation themselves. They can use a third-party DNS-service that does the validation, like Google Public DNS, or install DNSSEC capable (browser) software (plugins) on their computer. Applications that request a website, can also have built-in DNSSEC validation functionality.

A DNS-request transfers through multiple "delegation" levels. In addition to the signing of individual domain names, DNSSEC signatures also need to be inserted in these higher delegation levels, the 'root' and top-level domains (see Figure 2). This is not done by individual organisations, but by institutions who manage these parts of the internet. There is a direct technical dependency between collaborating

parties. The signing of all the levels involved in a DNS-request form together a so-called “chain of trust”.

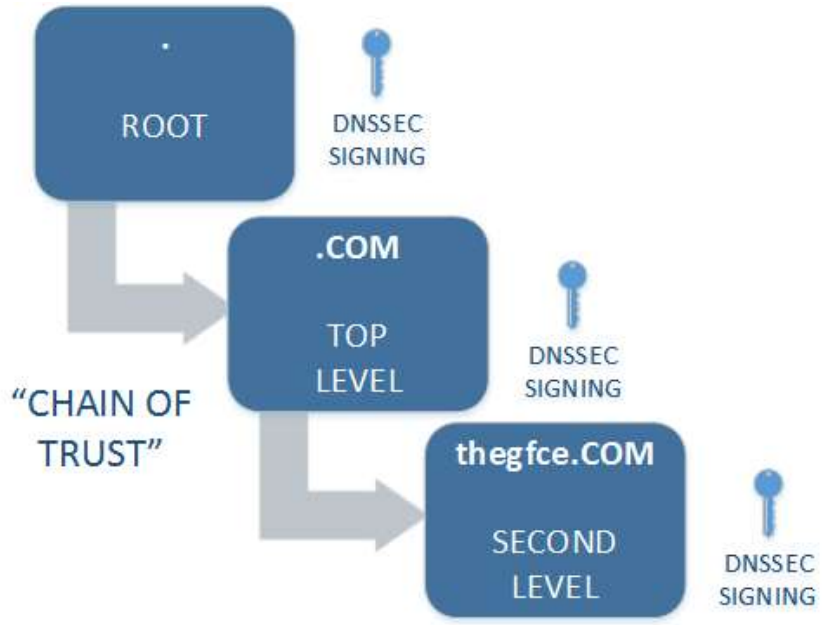

Figure 2. DNS-process ‘chain of trust’.

Further reading about DNSSEC can be found in (Surfnet, 2008 - 2009) as a more detailed and comprehensible tutorial.

What are the benefits?

Prevent cyber-attacks and economic loss. DNSSEC prevents forged DNS responses that can have a negative economic impact, because they can result in cyber-attacks leading to lost profits, fraud and damage to organisational reputation.

What are the challenges to adoption?

Technical challenges. To implement large-scale signing of (changes to) domain data requires automation of DNS(SEC) registration systems (IETF, 2017) which have proven to be challenging development projects.

Lack of understanding. In 2012, the Internet Society reported (York, Challenges and Opportunities In Deploying DNSSEC, 2012) that many technical infrastructure operators were not aware of DNSSEC operational guidelines and that it was not clear for most corporate or government IT-managers what the actual risk of the DNS vulnerabilities to his/her organisation are. In a more recent report of the

same author, it was noted that many of the challenges that were identified in 2012 are still valid (York, State of DNSSEC Deployment, 2016).

Chicken and egg-situation. In 2012, the Internet Society reported (York, Challenges and Opportunities In Deploying DNSSEC, 2012) that application developers and infrastructure operators wouldn't invest any effort in implementing DNSSEC because only few domains were signed, while domain holders had no intention to sign their domains because hardly any party validated DNSSEC signatures.

What's the current adoption status?

The adoption status for DNSSEC has two sides: the volume of DNSSEC signed domains and the validation of DNSSEC signatures.

The *deployment of DNSSEC signed domains* has made substantial progress since the root was signed in 2010. Most of the Top-Level Domains (e.g. .com, .de) have now been signed, while there are still some challenges with country-code domains, especially in developing countries. Technical barriers are being removed. For example, the major DNS servers now ship with DNSSEC capability, tools assisting DNSSEC operation are improving, and automation of DNSSEC provisioning is being improved (Switch, 2017). Further, new applications for DNSSEC are gaining traction, such as the use of DANE for TLS secured data transport in support of e-mail transfers. While there are still challenges in deploying and supporting DNSSEC, the above factors point to continued growth of signed domains with DNSSEC (Internet Society, 2016):

- 89% of generic top-level domains (.com, .net etc) zones have been signed.
- 47% of country-code top-level domains (.fr, .de etc.) have been signed
- Second-level domains (example.com etc) vary widely:
    - Over 2.5 million .nl domains have been signed (~45%), while in the Czech Republic even over 50% of the .cz-domains have been signed.
    - ~88% of measured zones in .gov have been signed.

Unfortunately, only ~0.5% of the .com domains -which represents a very large part of the internet- have been signed.

For *DNSSEC validation*, the deployment barriers and adoption drivers are different as is indicated by measurements from APNIC (APNIC, 2016). For example, many African and some of the Asian countries have (relatively) high DNSSEC validation rates because Google's Public DNS service (which applies DNSSEC validation) is being used by them. In North America, Comcast resolvers are a major validation

system; while in Scandinavia the increase in DNSSEC validation rates is also largely attributable to decisions of ISPs to switch on DNSSEC validation. Still, only approximately 14% of internet users around the world use DNSSEC-validating resolvers. Hence, to increase adoption of DNSSEC validation incentives should be directed towards private DNS service providers.

What is SPF, DMARC and DKIM?

The current e-mail system cannot prevent malicious actors sending forged e-mails on behalf of legitimate organisations. The e-mail address shown in the 'From' -field can be changed without any technical knowledge. It can therefore look like an e-mail that is send by 'info@ organisation.com', while in fact is it send by 'hacker@abadguy.com'. Without additional measures, there is no way to guarantee whether an e-mail was sent from the mentioned e-mail address. This makes it difficult to detect and filter phishing e-mail. A way to prevent e-mail spoofing is by validating the identity of the sender or of the sending e-mail server. This is called e-mail authentication. SPF, DKIM and DMARC are techniques providing the means for this type of authentication. They need to be implemented by individual organisations by adding elements to the DNS system and installing specific software on the e-mail server.

Sender Policy Framework (SPF): is a technique through which an organisation can specify which e-mail servers are authorised to send e-mails on behalf of this organisation. For example, the e-mail server used by a malicious actor sending a phishing e-mail from 'hacker@gmail.com' is not authorised to use 'info@organisation.com' in the 'From'-field of the e-mail. This can therefore be detected by spam filters of the receiving organisations.

DomainKeys Identified Mail (DKIM): is a technique through which an e-mail is signed with a digital signature. Just like with SPF, this enables the authentication of the sender, but in this case digital signatures are used to authenticate individual e-mail messages. Additionally, it also ensures that the message is not forged by a third party while it was in transit. It thereby protects the privacy and integrity of the content of the e-mail.

Domain-based Message Authentication, Reporting, and Conformance (DMARC): enables an organisation to publish the authentication mechanisms that it uses and additional functionalities. It provides information to (the devices of) users about how to handle e-mail messages that fail to be authenticated. It also specifies how identified domain misuse or errors in SPF and DKIM configurations

can be reported to the responsible organisation. Moreover, a policy can be specified on how receivers should handle failing messages.

What are the benefits of using these three standards?

Anti-phishing & e-mail-spoofing. SPF, DKIM and DMARC prevent e-mail spoofing, ensuring that legitimate e-mail addresses cannot be used as the shown sender of phishing e-mail. This makes phishing e-mails easier to detect by its recipients.

Brand protection. As the domain names of organisation cannot be abused anymore for distributing phishing e-mails, the use of these three standards prevent damage to the reputation of the domain owner.

What are the challenges to adoption?

Resources. It takes and requires the proper skills to properly understand, implement and configure these standards. A plan-do-check-act cycle needs to be established, involving multiple stakeholders within an organisation, to iteratively monitor the e-mail streams and to adjust the configurations accordingly.

What's the current adoption status?

An indication of the adoption status of DKIM, SPF and DMARC can be obtained by scanning the fraction of 'popular' websites that have published data that is needed for the execution of these protocols. One of these scanning tools (Eggert, 2017) reports that for 50 'popular' sites around the world the number of sites including SPF, DKIM or DMARC data are 36, 24 respectively 41. Although these numbers merely provide an indication for several 'popular' sites, they do indicate that around 50% or more of those popular sites have prepared for implementation of these protocols. For DMARC it is notable that a strong deployment increase has occurred in the first quarter of 2017.

In 2015, Return Path analysed more than 1,000 organisations across 33 countries. They found that, globally, only 22% of these organisation were publishing a DMARC record (Return Path, 2016).
One year later, they looked at the same companies. They found that 29% of them are now publishing a DMARC record. North America has the highest overall adoption rate: 42%.

What is IPv6?

The Internet Protocol (IP) facilitates the communication between devices on the global internet. Every device has a unique identifier, an IP-address, to communicate with other devices. IPv4 is the currently most used version of IP and enables 4.3 billion IP-addresses. Nearly all of these addresses have already

been assigned despite the use of some technical tricks to delay the moment of shortage. The adoption of IPv6, which provides 340 trillion, trillion, trillion unique IP addresses, is therefore needed to scale-up the internet and connect more users and devices. IPv6 solves several security issues and technical limitations of IPv4, making the network connections more robust, efficient and secure.

Which stakeholders are involved?

There are four main groups of stakeholders involved in the adoption and deployment of IPv6. Network infrastructure (e.g. routers, firewall) and software (e.g. e-mail, ERP software) vendors need to modify existing products and services to incorporate IPv6 capabilities. They need to develop new products and services enabled by IPv6 functionality. ISPs need to update their internet provisioning network which is used for providing internet access to their users. Internet users, including organisations, government agencies and home-users, need to ensure that their internal network can handle the IPv6 enabled internet traffic. This includes the use of an IPv6-compliant network infrastructure, such as routers.

What are its benefits?

Improved internet connectivity. IPv6 does not only solve the problem of the address space, but also provides other technical benefits, such as a more efficient internet, built-in security and improved support for mobility. For example, Facebook has presented tests that show that IPv6 is on average 15% faster for devices on mobile networks in the US (Saab, 2015).

Business continuity and innovation. It will be impossible for additional Internet devices or services to be connected to the internet when all the IPv4-addresses have been assigned. Organisations which have not adopted IPv6 may face complications in the deployment of new applications. Also, IPv6 is an opportunity for the development of new services, such as real-time information (improved end-to-end connectivity), personalised mobile services (improved mobility) and internet of things (IoT). Organisations which have not adopted IPv6 will be unable to connect to IPv6-only users. In countries where the internet infrastructure is still in developing phase, there is an opportunity for organisations, service providers, and end-users to skip IPv4 implementation and immediately start using IPv6.

Decreased costs & lower complexity. The reasons given for IPv6 deployment vary. It often comes down to “save money and make the network simple” (ISOC, 2017). Since pools of free IPv4 addresses have become depleted, the cost of obtaining an IPv4 address is rising. IPv6 also simplifies network management (e.g. it eliminates the need to use network address translation – NAT) and has features that can be used against cyber-attacks. By adopting IPv6 now, network operators and users will avoid the costs of continuing to maintain legacy IPv4 services.

National economic growth. Internet address resources are essential to the functioning and evolution of the internet. National infrastructures that use IPv6 are better equipped to make use of the economic opportunities enabled by innovative domains, such as smart cities and smart grids.

What are the challenges to adoption?

Resources. Implementing IPv6 does require effort, skill, and resources. Software and hardware developers, network operators, end-users and other stakeholders, often need to make changes to their systems and services in order to implement IPv6.

Perceived lack of need. A factor that impedes the adoption of IPv6, is the perception that IPv6 does not have a specific "killer application". However, as available IPv4 addresses become scarcer, the costs of IPv4-addresses and IPv4-networks will increase to the point that they become larger than the costs of adopting IPv6. This will be a large motivational factor.

Technical challenges. Practical problems do exist, but they are manageable. For example, the interaction with multiple firewalls can be a problem in specific situations. While many organisations had a successful transition and deployment, the implementation of IPv6 at a large software company has been halted because of incompatible internal network infrastructure (ISOC, 2017).

What is the current adoption status?

Since the introduction of IPv6, its adoption has been moderate. Recently, the deployment of IPv6 is increasing around the world. According to (ISOC, 2017) IPv6 measurements by Google, Akamai and APNIC show that IPv6 has now emerged from the "Innovators" and "Early Adoption" stages of deployment and is moving into the "Early Majority". The IPv4 Market Group comments that it expects IPv6 user count to exceed 50% world-wide in 2019, and with that, the start of the decline of the IPv4 address market.

A relevant factor behind this uptake lies in the fact that Regional Internet Registries (RIRs) around the world have run out of IPv4-addresses (only new market entrants may be allocated addresses). This depletion drives hosting and network providers to charge higher prices for the use of IPv4-addresses, which makes the transition to IPv6 addresses economically attractive.

Besides the depletion of IPv4 addresses there are more and more individual organisations that take the step to promote the deployment of IPv6. For example, in Belgium two major ISPs decided to promote IPv6. A code of conduct, initiated by the Belgian regulatory body for telecommunication and postal services, to limit the use of network address translation (to enable more effective cyber forensics) has contributed to this decision. This has led to a relatively high IPv6 deployment rate in

Belgium (ipv6-test.com, 2017). Similarly, Reliance JIO in India carries more than two third of India's IPv6 traffic and their adoption of IPv6 boosted the country's IPv6 utilization to 20% of all traffic (ISOC, 2017).

References

Study Group on Advanced Use of Internet with IPv6. (2010). *Final Report.*

Al-Furaih, I. (2014). *IPv6 Promotion and Deployment in Saudi Arabia.*

APNIC. (2016, June). *A quick review of DNSSEC Validation in today's Internet.* Retrieved from labs.apnic.net: labs.apnic.net/presentations/store/2016-06-27-dnssec.pdf

Chalmers, S., & Degezelle, W. (2015). *Best Practice Forum on Creating an Enabling Environment for IPv6 adoption.*

CIO Council. (2012). *Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government.*

Corbitt, B. (2003, Vol. 2 Issue 3). Trust and e-commerce: a study of consumer perceptions. *Electronic Commerce and Applications*, pp. 203-215.

Council of the European Union. (2017, September). *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU .* Retrieved from europa.eu: data.consilium.europa.eu/doc/document/ST-12211-2017-INIT/en/pdf

DNSSEC-campaign-references: www.afnic.fr/en/products-and-services/services/dnssec-17.html, london50.icann.org/en/schedule/wed-dnssec/presentation-dnssec-eu-25jun14-en.pdf, www.norid.no/en/registrar/nytt/dnssec/DNSSEC-nyhetsbrev5/: www.sidnlabs.nl/downloads/presentations/SIDN-Labs-InternetNL-20160316.pdf.

Dutch Government. (2012, August 13). *Operation black tulip.* Retrieved from Rijksoverheid.nl: www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2012/08/13/black-tulip-update/black-tulip-update.pdf

Eggert, L. (2017). *"Global Deployment Monitor"*. Retrieved from eggert.org: eggert.org

Facebook. (2014, August 19). *Massive Growth in SMTP STARTTLS Deployment*. Retrieved from Facebook.com: https://www.facebook.com/notes/protect-the-graph/massive-growth-in-smtp-starttls-deployment/1491049534468526/

Felt, A. P., Barnes, R., King, A., Palrmer, C. B., & Tabriz, P. (2017). Measuring HTTPS Adoption on the Web. *Proceedings of the 26th USENIX Security Symposium* (pp. 1333-1334). Vancouver: Usenix.

Google. (2014, August 6). *HTTPS as a ranking signal*. Retrieved from Webmaster Central Blog: https://webmasters.googleblog.com/2014/08/https-as-ranking-signal.html

Google. (2017, October 20). *Encrypted traffic to and from Google*. Retrieved from Google.com: https://transparencyreport.google.com/safer-email/overview

Howav, A., Hemmert, M., & Kim, Y. J. (2010). Determinants of Internet standards adoption: The case of South Korea. *Elsevier*, 253-262.

ICANN. (2017). *Identifier Technical Health Indicators (ITHI)*. Retrieved from icann.org/ithi: www.icann.org/ithi

IETF. (2017). *About the IETF*. Retrieved from ietf.org: ietf.org/about

IETF. (2017, March). *Managing DS Records from the Parent via CDS/CDNSKEY*. Retrieved from IETF.org: https://tools.ietf.org/html/rfc8078

Internet Architecture Board (IAB). (2014, November 14). *IAB Statement on Internet Confidentiality.* Retrieved from iab.org: https://www.iab.org/2014/11/14/iab-statement-on-internet-confidentiality/

Internet Society. (2012, October 4). *The DANE Protocol – DNS-Based Authentication of Named Entities*. Retrieved from Internetsociety.org: https://www.internetsociety.org/resources/deploy360/dane

Internet Society. (2016, December 31). *State of DNSSEC Deployment 2016*. Retrieved from internetsoeciety,org: https://www.internetsociety.org/resources/doc/2016/state-of-dnssec-deployment-2016/

IPv6 Promotion Council. (2002, September). IPv6 Deployment in Japan - the way we accomplish - . Japan.

ipv6-test.com. (2017). *IPv6 in Belgium*. Retrieved from ipv6-test.com: ipv6-test.com/stats/country/BE

ISOC. (2014-2016). *Mutually Agreed Norms for Routing Security (MANRS)*. Retrieved from Routingmanifesto.org: https://www.routingmanifesto.org/manrs/

ISOC. (2017, May 25). *State of IPv6 Deployment 2017*. Retrieved from Internetsociety.org: www.internetsociety.org/resources/doc/2017/state-of-ipv6-deployment-2017

MEWC Malaysia. (2008). *National Strategic IPv6 Roadmap.*

Ministry of Science, ICT & Future Planning. (2014). *Expansion Roadmap to promote a New Internet Industry.*

Ministry of Science, ICT & Future Planning South Korea. (2014, March). Expansion Roadmap to Promote a New Internet Industry. South Korea.

National Cyber Security Centre. (2016). *Cyber Security Assessment Netherlands.*

Return Path. (2016). *DMARC Intelligence Report.*

Saab, P. (2015, September 14). *IPv6: It's time to get on board*. Retrieved from Facebook code: https://code.facebook.com/posts/1192894270727351/ipv6-it-s-time-to-get-on-board/

Surfnet. (2008 - 2009). *Hardening the internet - The impact and importance of DNSSEC.* Retrieved from Surf.nl: https://www.surf.nl/binaries/content/assets/surf/en/knowledgebase/2009/rapport_200909_hardening_the_internet_DNSSSEC.pdf

Switch. (2017). *Domain Names with DNSSEC*. Retrieved from nic.ch: https://www.nic.ch/statistics/dnssec/

Verisign Labs. (2012). *A Quantitative Comparison Between X.509 CA Verification and DANE Via Attack Surface Analysis.* Retrieved from Verisignlabs.com: techreports.verisignlabs.com/docs/tr-1120004-1.pdf

York, D. (2012). *Challenges and Opportunities In Deploying DNSSEC.*

York, D. (2012). Challenges and Opportunities In Deploying DNSSEC.

York, D. (2016, November 13). *State of DNSSEC Deployment.* Retrieved from Internet Society: https://iepg.org/2016-11-13-ietf97/IEPG-DNSSEC-Deployment-1.pdf

This document was drafted and developed in cooperation with TNO for the Global Conference on Cyberspace GCCS in India (2017). Many thanks to all others, especially those from the internet infrastructure community, who participated in the realisation of this document.


GFCE
Global Forum on Cyber Expertise