Certificate Authority Collapse

Regulating Systemic Vulnerabilities in the HTTPS Value Chain

Axel M. Arnbak & Nico A. N. M. van Eijk[1]
Universiteit van Amsterdam, Faculty of Law, Institute for Information Law

Abstract. Recent breaches and malpractices at several Certificate Authorities (CA's) have led to a global collapse of trust in these central mediators of Hypertext Transfer Protocol Secure (HTTPS) communications. Given our dependence on secure web browsing, the security of HTTPS has become a top priority in telecommunications policy. In June 2012, the European Commission proposed a new Regulation on eSignatures. As the HTTPS ecosystem is by and large unregulated across the world, the proposal presents a paradigm shift in the governance of HTTPS. This paper examines if, and if so, how the European regulatory framework should legitimately address the systemic vulnerabilities of the HTTPS ecosystem. To this end, the HTTPS authentication model is conceptualised using actor-based value chain analysis and the systemic vulnerabilities of the HTTPs ecosystem are described through the lens of several landmark breaches. The paper explores the rationales for regulatory intervention, discusses the proposed EU eSignatures Regulation and ultimately develops a conceptual framework for HTTPS governance. It apprises the incentive structure of the entire HTTPS authentication value chain, untangles the concept of information security and connects its balancing of public and private interests to underlying values, in particular constitutional rights such as privacy, communications secrecy and freedom of expression. On the short term, specific regulatory measures to be considered throughout the value chain includes proportional liability provisions, meaningful security breach notifications and internal security requirements, but both legitimacy and effectiveness will depend on the exact wording of the regulatory provisions. The EU eSignatures proposal falls short on many of these aspects. In the long term, a robust technical and policy overhaul is needed to address the systemic weaknesses of HTTPS, as each CA is a single point of failure for the security of the entire ecosystem.

Keywords: HTTPS, Cybersecurity, Internet Governance, Constitutional Values, E-Commerce, Value Chain Analysis, Security Economics, eSignatures Regulation.

WORK IN PROGRESS

DRAFT PREPARED FOR TPRC 2012, NOT FOR CITATION

[1] Author information: http://www.ivir.nl/staff/overview.html. Comments are gratefully received at a.m.arnbak@uva.nl

Table of Contents

1. Introduction 2
2. The HTTPS Authentication Ecosystem 4
  2.1 The Current HTTPS Authentication Model 4
  2.2 The HTTPS Market 6
  2.3 The Actor-Based HTTPS Value Chain 10
3. Systemic Vulnerabilities 11
  3.1 DigiNotar: Landmark Breach 11
  3.2 Multiple CA Breaches, History Repeating 15
  3.3 Systemic Vulnerabilities of the HTTPS Authentication Process 16
4. Governance 18
  4.1 Values Underlying HTTPS Governance 19
  4.2 The EU proposal for an eSignatures Regulation 22
  A) Underlying Values 23
  B) Scope 24
  C) Liability 25
  D) Security Requirements 26
  E) Security Breach Notification 27
  F) Supervision 28
5. Conclusion & Analysis: Regulating the HTTPS Value Chain 30

1. Introduction

Hypertext Transfer Protocol Secure ('HTTPS') has evolved into the de facto standard for secure web browsing. Through the certificate-based authentication protocol, web services and internet users protect valuable communications and transactions against interception and alteration by cybercriminals, governments and business. In only one decade, it has facilitated trust in a thriving global E-Commerce economy, while every internet user has come to depend on HTTPS for social, political and economic activities on the internet.

However, for years security experts have sounded the alarm bells about systemic vulnerabilities to the security of HTTPS communications. A successful attack on HTTPS requires the compromise of such a certificate and the ability to modify IP traffic,[2] and may lead to the compromise of sensitive information, such as private communications and financial data. In 2009, Ristić developed a threat model that included over fifty threats to the Secure Socket Layer ('SSL') ecosystem upon which HTTPS is built, calling it 'full of traps, each of which is very easy to fall into'.[3]

[2] Certificate compromise is extensively discussed in paragraph 3. Manipulating IP traffic may be achieved through a rogue hotspot, poisoning DNS/APR cache, malware or by accessing traffic at ISPs directly. Network providers, DNS servers and governments may have this type of access, while it is a relatively straightforward affair for cybercriminals.

[3] See: http://blog.ivanristic.com/2009/09/ssl-threat-model.html. See also C. Soghoian & S. Stamm, Certified Lies: Detecting and Defeating Government Interception Attacks Against

One of the prominent threats has been the HTTPS authentication ecosystem that mediates the trust relationship between web site operators,[4] Certificate Authorities ('CA's') that issue SSL certificates, web browsers and end-users. The 2011 security breach at Dutch CA Diginotar exposed the 'fundamental weaknesses in the design of HTTPS' to a global audience.[5] Other breaches or malpractices at larger CA's such as Comodo, VeriSign and Trustwave have added to a collapse of trust in HTTPS communications. Worryingly, while serving as the de facto standard for secure web browsing, in many ways the security of HTTPS is broken.

The HTTPS ecosystem is by and large unregulated,[6] but has become a top priority in telecommunications policy given our increasing dependence on secure web communications. Partly in response to the breach at Diginotar, European policymakers suggested a review of the EU Electronic Signatures Directive that pioneers a legal framework for HTTPS in June 2012. Upon adoption, the proposed eSignatures Regulation acquires immediate binding force in the legal systems of 27 Member States, impacting global HTTPS governance substantially. Thus, the proposal currently under consideration is one to watch.

Against this background, this paper examines if, and if so, how the European regulatory framework should legitimately address the systemic vulnerabilities of the HTTPS ecosystem. Apart from discussing the proposed Regulation, we aim to conceptualise the ecosystem for legal analysis and further scholarship on HTTPS governance. Our findings should thus be relevant for anyone interested in HTTPS, cybersecurity and internet governance – both in Europe and abroad.

The paper sets out to conceptualises the HTTPS authentication ecosystem in paragraph 2. Several landmark breaches at CA's inform a description of the systemic vulnerabilities of the HTTPS ecosystem in paragraph 3. The rationales for regulatory intervention are explored in paragraph 4.1. This informs our assessment of the proposed Regulation, which we discuss along the lines of several pressing themes. Finally, the paper goes beyond the EU proposal to offer general insights on legitimate HTTPS governance in a concluding paragraph 5.

The paper is among the first legal analyses of the HTTPS ecosystem. Both descriptive and normative legal research is conducted. The paper adopts an external perspective as it researches a problematic societal status quo and the viability of (not yet existing) regulation to overcome this. In doing so, it adopts value chain analysis to expose the incentives and interactions of its various stakeholders. The research method applied is primarily desk research. The legal analysis derives inspiration from leading security economics and information security scholarship. As this paper is a part of a four year Ph.D. project on the regulation of communications security,

SSL, Financial Cryptography and Data Security '11, March 2011, para. 2.3 and N. Vratonjic, J. Freudiger, V. Bindschaedler, J.Hubaux, The Inconvenient Truth about Web Certificates, working paper, Workshop on the Economics of Information Security 2011, para. 2.2.

[4] This group includes websites (HTTPS) and web services (such as POP/IMAP). For ease of reading, we mostly use 'HTTPS' and 'web sites' throughout the paper.

[5] ENISA (authors from PDF metadata: G. Hogben & M. Dekker), 'Operation Black Tulip: Certificate Authorities Lose Authority', version 2, Dec. 2011, http://www.enisa.europa.eu/media/news-items/operation-black-tulip/view

[6] See paragraph 4.

conducted by the authors, the analysis may be complemented with other (qualitative) research methods in future versions, such as expert interviews and workshops.

HTTPS has many facets. We focus on the legal aspects of the authentication process between the end-points of HTTPS communication, usually a website and an end-user. This paper is not about the governance of the cryptographic channel that is set up after successful authentication. The cryptographic protocols underlying HTTPS are only mentioned insofar they impact the authentication process. Furthermore, we analyse the unregulated SSL certificate environment, through which the vast majority of HTTPS communications are mediated, rather than the partly regulated ‘qualified certificate’ ecosystem. This regime is briefly discussed in para. 3.1, because DigiNotar was both a non-qualified SSL certificate and a qualified certificate provider.

2. The HTTPS Authentication Ecosystem

When internet communications became available outside of early adopting communities and were quite enthusiastically adopted by millions of end-users, the confidentiality and integrity of these communications emerged as important issues. These issues are purportedly tackled with HTTPS communications. This paragraph describes the HTTPS Authentication Trust Model, the HTTPS market and subsequently maps the actor-based HTTPS Authentication Value Chain to conceptualize the interactions between key stakeholders.

2.1 The Current HTTPS Authentication Model

HTTPS communications facilitate end-user authentication of web services and encrypted communications between them. Essentially, HTTPS is a two-step process: first, a trust relationship (a ‘handshake’) is established between the website and web browser of the end-user, providing authentication. Secondly, successful authentication leads to a TLS/SSL encrypted channel between the website and browser (a ‘tunnel’).[7] This tunnel protects against third party eavesdropping (confidentiality) and alteration (integrity) of information, by securing the communications channel from endpoint to endpoint – from web service to end-user browser, and vice versa. The handshake authentication thus serves as the stepping stone for the confidentiality and integrity that HTTPS seeks to deliver. As Roosa & Schultze observe, ‘the degree of security provided by SSL rises and falls with the authentication system upon which it rests.’ [8] This paper focuses on this authentication process between website and the end-user’s web browser.

[7] R. Anderson, Security Engineering: Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley: Indianapolis 2008, p. 670.

[8] S. Roosa & S. Schultze, ‘The "Certificate Authority" Trust Model for SSL: A Defective Foundation for Encrypted Web Traffic and a Legal Quagmire’, *Intellectual Property & Technology Law Journal*, Volume 22, Number 11, November 20 I0, p. 3.

If a website or service wants to provide HTTPS, it needs to obtain an SSL certificate from a CA. Basically, these SSL certificates are small computer files that might contain information on hostname (website), certificate owner (website), certificate issuer (CA), validity period and public key.[9] The amount of information that SSL certificates provide depends on the type of certificate purchased by its owner. Domain Validated (DV) certificates can be acquired at low costs and may require a website operator to reply to an e-mail sent by the CA to a standard e-mail address in the WHOIS database for domain validation.[10] The various types of Extended Validation (EV) certificates require more thorough validation by the CA, for example by phone, written letter or face-to-face, verifying both domain and the organization behind it.[11] If validation succeeds, CA's sign the EV certificate.[12]

Every time an internet user visits to a particular website, his browser requests the site to identify itself. Upon receiving such a request, the server of the website responds by either offering no information (standard unencrypted communications over HTTP) or a copy of its SSL certificate to the browser. If a browser receives an SSL certificate, it sets out to check if it trusts the issuing CA. In the case of untrusted CA's (or self-signed certificates that seek an SSL connection), the browser may give the end-user a security warning of an 'untrusted connection'. If the browser does trust the issuing CA, it subsequently aims to prove that the public key assigned to the SSL certificate matches with the certificate of the issuing CA. If this second test succeeds, a chain of trust is established: through the SSL certificate issued and signed by a trusted CA, the browser trusts that the domain name and the server it directs to actually belong to the same entity. After a successful authentication process, the encrypted tunnel between website and end-user is set up. Browsers notify users of a successful handshake, either by displaying a padlock, changing colours in the location bar or some other conspicuous area of their browser.

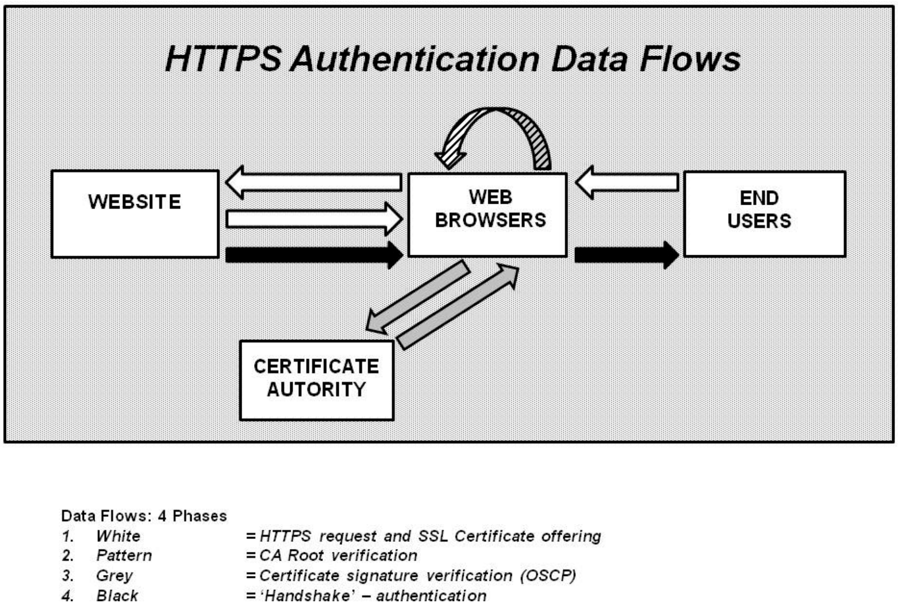
The described data flows are visualised below:

[9] Anderson 2008, p. 672.

[10] CA/Browser Forum, Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, version 1.0, effective 1 July 2012. See: http://www.cabforum.org/Baseline_Requirements_V1.pdf

[11] CA/Browser Forum, Guidelines For The Issuance And Management Of Extended Validation Certificates, version 1.4, effective 29 May 29 2012, see: http://www.cabforum.org/Guidelines_v1_4.pdf

[12] See: https://freedom-to-tinker.com/blog/sjs/firefox-changes-its-https-user-interface-again/


HTTPS Authentication Data Flows
WEBSITE
WEB BROWSERS
END USERS
CERTIFICATE AUTORITY
Data Flows: 4 Phases
1. White = HTTPS request and SSL Certificate offering
2. Pattern = CA Root verification
3. Grey = Certificate signature verification (OSCP)
4. Black = 'Handshake' – authentication

2.2 *The HTTPS Market*

Since the inception of the HTTPS authentication process with the advent of the Netscape browser in the 1990s, a vibrant market for HTTPS communications emerged. This market involves roughly four direct stakeholders: i) web site operators or other subscribers; ii) certificate authorities; iii) web browsers, and iv) end-users.[13]

Websites come in every form imaginable. It is up to them to deploy HTTPS. Deploying HTTPS may be achieved at low costs and sends out a message that end-users can entrust the website with valuable information, such as personal data, private communications and financial transactions. In E-Commerce and electronic communications – web-based e-mail, online banking, social networking – HTTPS deployment is surely on the rise. For example, Internet giants such as Google, Facebook and Skype employ HTTPS on the login sections of their websites, while enabling the use of HTTPS on their entire websites.

Research on HTTPS deployment is still in its infancy. Vratonjic et. al. suggest that around one-third of the internet's 1 million most popular web pages can be browsed with HTTPS.[14] US based security firm Qualys calculated 10% of the 1

[13] Roosa & Schultze 2010, p.4. Subscribers is a somewhat broader and more accurate term for web site operators, as buyers of certificates do not necessarily have to be website operators. For ease of reading, this paper will use the terms websites or web site operators.

[14] Vratonjic 2011, p. 3.

million most popular sites.[15] A notable drawback for websites to deploy HTTPS is that embedded content – third party ads, feeds, widgets and tracking networks – may not support HTTPS,[16] in which case the advantages of HTTPS are lost.[17] In any event, non-encrypted embedded content on a HTTPS website will spur a security warning ('some parts of this site are not trusted, should we only show secure content?'), which lets users negate the third party content. So if embedded content is a part of the revenue model of a site, which is the case with many websites, it has strong incentives not to deploy HTTPS.[18]

HTTPS deployment is not a binary affair, in the sense that a website provides it, or does not. Website operators have many options for implementing HTTPS that have a consequent impact on the level of security provided. These implementation options include the type of SSL certificate purchased, whether the certificate is still valid or expired, whether the latest encryption (TLS/SSL) standards are supported, which parts of the website employ HTTPS, and so forth. Vratonjic et al. found that 'only 16% of the websites implementing HTTPS carry out certificate-based authentication properly'.[19] SSL Pulse, a project run by Qualys,[20] surveyed the 185.000 most popular HTTPS websites on the internet. The project finds that only 13% offer end-users (what Qualys calls) 'genuine security',[21] only 8% use EV certificates and less than 1% support the HTTP Strict Transport Security protocol, in effect forcing browsers to communicate with the site through HTTPS. These numbers should not be interpreted exactly, but render it safe to observe that the state of HTTPS implementation is sub-optimal from a security perspective.

Certificate Authorities have a critical role in the HTTPS ecosystem, as they facilitate the handshake between websites and browsers. They may be distinguished in three categories: Root CA's, intermediate/subordinate CA's and untrusted CA's.[22] Root CA's are trusted by default by browsers, after they have solicited for such a status with the browsers and complied with the varying browser CA trust policies. Intermediate/subordinate CA's are either directly verified by one Root CA or part of a chain of trust of several intermediate CA's that ultimately ends with one Root CA. Interestingly, both Root CA's and intermediate CA's that are part of such a chain of

[15] Qualys presentation at 2012 RCA Conference, slide 32, using Alexa's Top 1 million sites: https://community.qualys.com/servlet/JiveServlet/download/38-9096/SSL_and_Browsers-The_Pillars_of_Broken_Security.pdf

[16] Google AdSense: https://support.google.com/adsense/bin/answer.py?hl=en&answer=10528

[17] For example, unencrypted third party content may run JavaScript or CSS and have access to session cookies. In this scenario, third parties have access to the sensitive information HTTPS aims to protect.

[18] An interesting account of this dynamic can be found here: http://arstechnica.com/business/2011/03/https-is-great-here-is-why-everyone-needs-to-use-it-so-ars-can-too/, and in A. Langley, 15 July 2012 HOPE9 talk, 'mixed scripting' section: http://www.imperialviolet.org/2012/07/19/hope9talk.html

[19] Vratonjic 2011, p.3: "i.e. using trusted, unexpired certificates with valid signatures, deployed on proper domains."

[20] See https://www.trustworthyinternet.org/ssl-pulse/

[21] From the SSL Pulse website: "To be secure, a site has to be well configured, which means that it must have the A grade. In addition, it must not be vulnerable to any of the two currently known attacks against SSL (Insecure Renegotiation and the BEAST attack)."

[22] Soghoian & Stamm 2010, p. 2.

trust are treated equally by browsers, leading to a successful authentication. Untrusted CA's or self-signed (by the owner of a website) certificates evoke the 'untrusted connection' security warning when they offer browsers an SSL connection.

A crucial characteristic of the HTTPS Trust Model is that any CA can sign SSL certificates for any domain name. For example, a domain name holder – say Google in the case of www.google.com – possesses an SSL certificate for his domain. This doesn't stop anyone in stepping to any CA and request another SSL certificate for www.google.com, even though this other CA is not the CA that Google approached to sign its SSL certificate. From the CA perspective, there are institutional limits to issuing this particular certificate (validation procedures), but no technical ones. So if one obtains this second certificate with a CA that has root status, browsers will trust the alternate certificate by default. End-users will get the familiar HTTPS notification, without noticing whether their HTTPS communications are mediated by the Google-owned certificate or the second certificate. This ability to sign for any domain name has profound implications for the security of the HTTPS ecosystem, long recognized in the security community.[23] It was exploited with a host of SSL certificates, including for the google.com domains, in a number of breaches, including the DigiNotar breach.

From a business perspective however, the position in the ecosystem and the fact that CA's can sign for any domain name is attractive.[24] The CA industry has flourished over the last decade, as it is relatively easy to set up your own CA and buy yourself into a chain of trust.[25] Nobody knows its size or the exact number of CA's in the market. Data from the Electronic Frontier Foundation SSL Observatory suggests that approx. 650 organizations spread over more than fifty jurisdictions have either root or intermediate status with Mozilla or Microsoft.[26] This number includes governments, as more than 50 own CA's.[27] In addition, many root CA's own multiple subordinate CA's, that may partake in the aforementioned chain of trust and in that case enjoy default trust by browsers. This practise enables root CA's to divide operations in various market segments and compete with other CA's on price differentiation, as many websites don't seek high security certificates, but cost-effective ones.[28]

Web browsers are another critical stakeholder in HTTPS communications. As the interface between end-users and HTTPS communications, browsers interact with websites, CA's and the end-user. In particular, the HTTPS ecosystem relies upon browsers to establish whether a particular CA can be entrusted root status and to check the validity of certificates (on trust revocation, see below). Furthermore, it

[23] Roosa & Schultze 2010, p. 5. Soghoian & Stamm 2010.

[24] Roosa & Schultze 2010, p. 4 and footnote 8-10. There are numerous webpages that describe how to become a CA around, for example: http://technet.microsoft.com/en-US/library/ff849263%28v=ws.10%29.aspx

[25] Roosa & Schultze 2010, p. 3.

[26] See: https://www.eff.org/observatory

[27] According to EFF's SSL Observatory data, see https://www.eff.org/files/countries-with-CAs.txt

[28] Schultze 2010, p. 6; Vratonjic 2011, p. 31/32.

notifies successful authentication and the establishment of encrypted tunnels to the end-user.[29]

In determining whether CA's should be granted root status, browsers have developed different trust policies. This has lead to a different number of root CA's per browser. Mozilla's Firefox browser maintains its own public database, containing approx. 150 CA's.[30] Microsoft's Root Certificate Program is tied to the Windows operating system and lists around 320 CA's.[31] Similarly, the Apple Root Certificate Program is connected to OS X and has approx. 190 CA's in its database.[32] The Google Chrome browser uses the respective lists of the operating systems it is installed upon, while retaining a right to remove any CA from these lists.[33] Meanwhile, the Google Checkout API lists approx. 170 trusted root CA's.[34] Each of these datasets contains several government CA's from all over the world. Moreover, we have seen that default trust is bestowed upon intermediate CA's whenever they partake in a chain of trust containing one root CA.

In the case of (or if there is reason to suspect) certificate or even CA compromise, swift trust revocation is essential to minimise the associated risk. For certificates, all major browsers employ Online Certificate Status Protocol (OCSP) responders. These are operated by CA's and let browsers check whether trust in a certain certificate has been revoked. For CA revocation, browsers need to alter aforementioned root CA lists and patch the browser software, which end-users subsequently need to update to take effect. An important drawback of OCSP effectiveness, is that its use by CA's is not mandatory and often overruled in order to maintain connectivity between a web service and users.[35]

End-users have an interest in seeking HTTPS communications with websites, as it is their valuable information that is on the line. However, users depend to a large degree on security decisions made by the aforementioned stakeholders. Websites initiate HTTPS communications through SSL certificates, that are validated and signed by CA's and verified by browsers. End-users don't interact directly with CA's.[36]

[29] The notification depends on the type of browser the end-user has installed on his device. The notifications vary from browser to browser, making it difficult for the average user to recognise succeeded authentication and base decisions-making on pursuing the connection with that particular website: https://freedom-to-tinker.com/blog/sjs/firefox-changes-its-https-user-interface-again/

[30] For Mozilla: https://www.mozilla.org/projects/security/certs/

[31] For Microsoft: https://social.technet.microsoft.com/wiki/contents/articles/2592.asp

[32] For Apple: https://www.apple.com/certificateauthority/ca_program.html

[33] For Chrome: http://www.chromium.org/Home/chromium-security/root-ca-policy

[34] For Google Checkout certificate trust policy, visit: https://support.google.com/checkout/sell/bin/answer.py?hl=en&answer=134466&from=57856&rd=1

[35] Langley 2012, 'Therefore online revocation checks which result in a network error are effectively ignored', see: http://www.imperialviolet.org/2012/02/05/crlsets.html. Furthermore, Langley notes that the OSCP-check gives rise to privacy concerns, as it informs CA's which IP-addresses request the validity a particular certificate, in effect exposing what websites are visited by which IP-addresses.

[36] ENISA 2011, p. 2. In particular footnote 5, which refers to the New Zealand BankDirect case, in which 299 in 300 users dismissed security warnings. Also Vratonjic 2011, p.32.

End-users that want to influence the HTTPS authentication process, need basic knowledge of HTTPS technology, sufficient information about security levels at these other stakeholders and insight in the consequences of a communications compromise. Their options are limited: they can choose which browser software and web services to trust, while balancing their security interests with other parameters, such as usability, pricing and features.[37] Only a very small margin of technically savvy users might pursue an (indirect) relationship with CA's through browser preferences, for example by blocking all certificates provided by a certain CA.

A common practise for CA's is to disclaim liability for losses suffered as a cause of reliance in certificates.[38] Roosa & Schultze observe that CA's 'place onerous technical obligations [...], such as being familiar with cryptographic protocols and making independent judgements about the trustworthiness of any given digital certificate' on end-users.[39] For this to happen, an end-users needs to check whether an SSL connection is established between a website and a browser, then check the digital certificate that is offered, examine the certificate and the associated CA, and ultimately judge whether their trust is justified. Users seeking the required information to evaluate the legal consequences of placing their trust in a certain certificate and its issuing CA, are in for something. After analysing the certificate, users need to browse to the CA website, pick the relevant legal document out of dozens available in legal repositories of CA's (often 'the relying party agreement' and the applicable contract of the type of certificate in question), read and analyse the legal writing, and ultimately balance their trust decisions against aforementioned factors of price, usability and connectivity. In this context, the average end-user cannot reasonably be expected to exert control over the HTTPS ecosystem.[40]

2.3 The Actor-Based HTTPS Value Chain

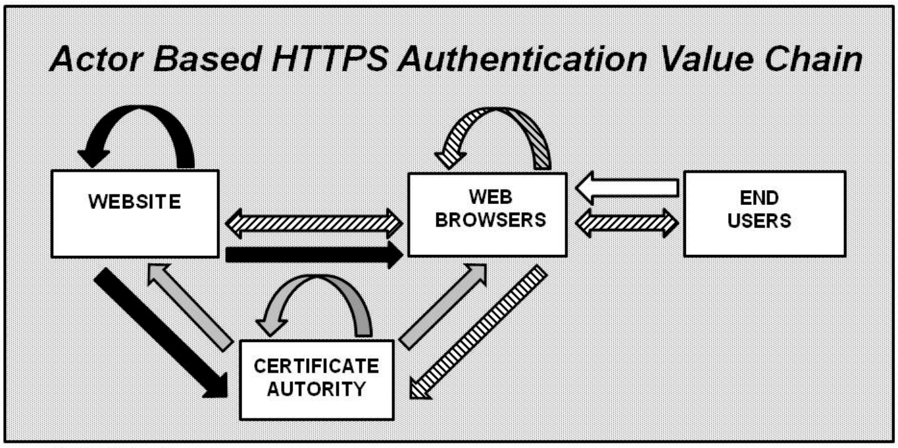
Now that the authentication process, it's data flows and the market characteristics for HTTPS have been described, an actor-based value chain for the HTTPS ecosystem can be mapped. This conceptualisation helps to understand the interactions between the different actors, or stakeholders, and the impact of these interactions on secure communications throughout the ecosystem. Here, 'value' is not understood as the flow of economic value between stakeholders, but rather as the flow of communications security practises. In other words, the communications security value that different stakeholders add to the system. This conceptualisation should help to expose potential dependencies and weaknesses of HTTPS from a communications security perspective. Departing from solely economic value, our value chain helps to understand the broader values at stake (see para. 4.1), rather than than market incentives alone. The value chain is visualised below:

[37] Users may add https to the url of these sites, or order their browsers to look for the availability of HTTPS through the settings menu or by installing a browser add-on such as HTTPS everywhere or Force TLS/SSL.

[38] Vratonjic 2011. Roosa & Schultze 2010, p. 6. We will return to recent developments on liability issues in our analysis of the CA/Browser Forum initiatives in paragraph 4.

[39] Roosa & Schultze 2010, p. 7.

[40] ENISA 2011, p. 2.



HTTPS Value Flows

1. End User (white)	*= HTTPS Request, Valuable Information*
2. Browser (pattern)	*= Verification of CA Root Application*
	= Verification of Certificate (incl. OSCP request to CA)
	= HTTPS Communication Conduit
3. CA (grey)	*= CA Root Status Application with Browsers*
	= SSL Certificate sale to Website
	= OCSP Responses to Browsers
	= Certificate Revocation and Internal Security
4. Website (black)	*= SSL Certificate purchase with CA*
	= SSL Certificate offering to browser
	= SSL server implementation

We analyse the HTTPS value chain from a regulatory perspective and its implications for governance in paragraph 4. The next paragraph describes the systemic vulnerabilities of the HTTPS ecosystem in theory and in practise, based on above conceptualisation of the HTTPS value chain.

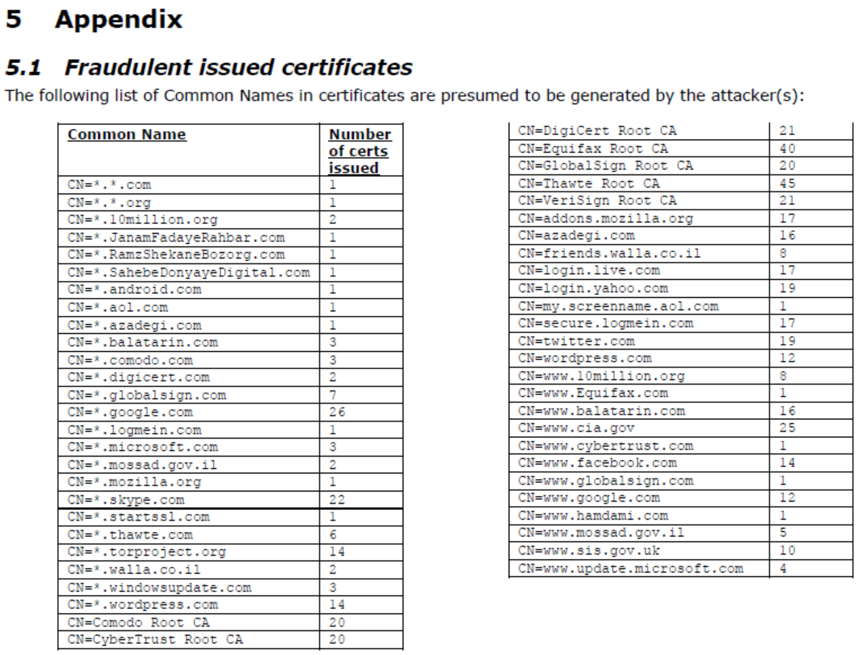
3. Systemic Vulnerabilities

This sections presents an overview of the systemic vulnerabilities of the HTTPS ecosystem. A theoretical perspective is derived from literature review of the scientific and other expert communities, while an analysis of the well-documented landmark breach at Dutch CA DigiNotar gives practical insight into the systematic vulnerabilities of the HTTPS trust model. This practical perspective is complemented with a description of several other breaches at CA's. We start with breach at DigiNotar, because it is the only breach that has been extensively documented in its aftermath and because of its worldwide significance and media coverage, despite the marginal size of the CA.

3.1 DigiNotar: Landmark Breach

On Friday 2 September 2011, towards midnight, a bar appeared at the top of Dutch television screens announcing an extra news broadcast at 1 AM. Viewers were in for a somewhat surrealist scene. Piet Hein Donner, the Minister of the Interior, sitting all by himself at an ordinary little table, read out a statement: the internet was no longer safe. But the world could rest assured and go quietly back to sleep; adequate measures had been taken. The Dutch Government had saved the country, and the internet.

The Ministerial assurances marked the beginning of the DigiNotar affair, which ultimately resulted in the CA's bankruptcy.[41] The affair was triggered by unauthorized access, reportedly by Iranian hackers, to the CA capacity of DigiNotar. As early as mid July 2011, DigiNotar knew that their systems had been hacked. For nearly two months, the CA managed to conceal the breach. But it was not before late August that the Dutch CERT Govcert.nl,[42] received a report from a German sister organization that something was probably wrong: an Iranian Internet user posted on a public forum that he wanted to surf to Google.com, but received a message about a possible fraudulent certificate. Later, it emerged that in this long period of obscurity, hundreds of false certificates had been created, the list of which is quite alarming. From the forensic report:[43]



5 Appendix

5.1 Fraudulent issued certificates

The following list of Common Names in certificates are presumed to be generated by the attacker(s):

Common Name	Number of certs issued
CN=*.*.com	1
CN=*.*.org	1
CN=*.10million.org	2
CN=*.JanamFadayeRahbar.com	1
CN=*.RamzShekaneBozorg.com	1
CN=*.SahebeDonyayeDigital.com	1
CN=*.android.com	1
CN=*.aol.com	1
CN=*.azadegi.com	1
CN=*.balatarin.com	3
CN=*.comodo.com	3
CN=*.digicert.com	2
CN=*.globalsign.com	7
CN=*.google.com	26
CN=*.logmein.com	1
CN=*.microsoft.com	3
CN=*.mossad.gov.il	2
CN=*.mozilla.org	1
CN=*.skype.com	22
CN=*.startssl.com	1
CN=*.thawte.com	6
CN=*.torproject.org	14
CN=*.walla.co.il	2
CN=*.windowsupdate.com	3
CN=*.wordpress.com	14
CN=Comodo Root CA	20
CN=CyberTrust Root CA	20
CN=DigiCert Root CA	21
CN=Equifax Root CA	40
CN=GlobalSign Root CA	20
CN=Thawte Root CA	45
CN=VeriSign Root CA	21
CN=addons.mozilla.org	17
CN=azadegi.com	16
CN=friends.walla.co.il	8
CN=login.live.com	17
CN=login.yahoo.com	19
CN=my.screenname.aol.com	1
CN=secure.logmein.com	17
CN=twitter.com	19
CN=wordpress.com	12
CN=www.10million.org	8
CN=www.Equifax.com	1
CN=www.balatarin.com	16
CN=www.cia.gov	25
CN=www.cybertrust.com	1
CN=www.facebook.com	14
CN=www.globalsign.com	1
CN=www.google.com	12
CN=www.hamdami.com	1
CN=www.mossad.gov.il	5
CN=www.sis.gov.uk	10
CN=www.update.microsoft.com	4

[41] For more information, ENISA (authors from PDF metadata: G. Hogben & M. Dekker), 'Operation Black Tulip: Certificate Authorities Lose Authority', version 2, Dec. 2011, http://www.enisa.europa.eu/media/news-items/operation-black-tulip/view and the forensic report by security firm Fox-IT, DigiNotar Certificate Authority breach, public report version 1, 5 Sep. 2011 http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1.html

[42] Govcert.nl is now part of the Dutch National Cyber Security Centre (NCSC) (see: www.govcert.nl and www.ncsc.nl). A file on DigiNotar can be found on the Govcert website.

[43] Fox-IT 2011, p. 10.

DigiNotar had root status with all mayor browser vendors, which consequently trusted all these corrupt SSL certificates by default.

Apart from these SSL certificates, DigiNotar provided ‘qualified certificates’ and was one of six providers of ‘PKI Overheid’, the Dutch government accredited Public Key Infrastructure (PKI) certificates. In contrast with SSL certificates, these certificates are regulated by the 1999 EU Electronic Signatures Directive – which contains provisions on liability and security practises [44] – and its much stricter implementing provisions in the Dutch Telecommunications Act, notably on security requirements and auditing obligations.[45] Their use is mandated by law in several situations, for instance when the government communicates with citizens (tax assessment, implementation of employee insurance schemes, DigiD) and in the private sector, for civil-law notaries and bailiffs to place or alter entries in the land register.

The forensic report illuminated that the security practises at DigiNotar were in a terrible state. The software of its servers had not been patched, logging was insufficient, and DigiNotar had no anti-virus protection in place. Moreover, all (qualified, root and subordinate) CA servers were members of the same Windows domain, leaving critical systems and functionalities accessible over the same Local Area Network, which was secured with a weak password (Pr0d@dm1n),[46] that was ease to crack with the hacker tools that were found afterwards on the DigiNotar systems.[47] Notably, EU and Dutch regulations had not quite resulted in compliance with DigiNotar’s qualified certificate operations. In this respect, the CA had successfully passed several periodic auditing procedures (for the issuance of EV certificates and Qualified signatures) that are ETSI standardised.[48]

The damage was probably enormous, but cannot be determined with certainty. Based on the logging of OCSP requests at DigiNotar, the HTTPS communications of reportedly 300.000 different IP-addresses were intercepted; at least, this number of IP-addresses reportedly used a fraudulent SSL certificate for google.com for a period of weeks.[49] According to the forensic report, the breach

[44] Directive 99/93/EC, OJ L 13/12 of 19 January 2000. On liability: art. 5 sub [2], in case the CA fails to revoke a certificate on request of its subscriber, on CA and certificate security requirements: art. 2 sub [10] jo. appendix I & II.

[45] *Kamerstukken II*, 2000/01, 27.743; Statute Book 2003, 199 (Electronic Signatures Act) in art. 18.15 (security requirements) and art. 18.16 (auditing obligations) of the Dutch Telecommunications Act, to be found via (Dutch only): http://wetten.overheid.nl/BWBR0009950/volledig/geldigheidsdatum_09-08-2012#Hoofdstuk18_Artikel1815.

[46] See: http://www.wired.com/threatlevel/2011/09/diginotar-bankruptcy/

[47] Fox-IT 2011, p. 8-9. The physical security was in perfect state, peculiarly, as the servers stood in highly expensive a tempest proof room.

[48] From ENISA 2011, p. 1: “Diginotar was audited yearly by an independent auditor against the ETSI standard (TS101456) for certificate authorities” and p. 2: “The Diginotar website until recently showed an audit report stating that “the management system for issuance of certificates of DigiNotar complies with ETSI TS 101 456 (v. 1.4.3) - normalized certificate polices NCP+, EV specified in ETSI TS 102 042 (v. 2.1.2).”

[49] Fox-IT 2011, p. 8.

probably targeted Iranian private communications, as analysis of IP-addresses from the OCSP responder suggests that 99% of the 300.000 IP-addresses were based in Iran. But this number is contentious, as OSCP requests are not mandatory, and could have been blocked or even faked by the attackers.[50] Furthermore, it should be noted that one IP-address doesn't correspond with one user, although the number of 300.000 users is frequently mentioned in media reports. ENISA speaks of 'millions of citizens' and notes that some experts believe that the lives of Iranian activists have been put at risk.[51] These claims cannot be confirmed nor denied, but attest to the seriousness of the breach. In addition to aforementioned 300.000 Iranians, researchers cannot rule out the possibility that undetected rogue certificates have been produced in the Qualified and PKI Overheid environments.[52] Therefore, the entire range of DigiNotar activities could have been compromised and already released certificates could no longer be trusted.

At the nocturnal press conference, Minister Donner announced several mitigation measures. Firstly, the 'operational management of DigiNotar was transferred', in other words the government had taken control of operations while DigiNotar still had root CA status with several browsers. Secondly, a process was started for a transition to other certificate suppliers. Notably, the process opted for was one of gradual transition to safeguard continuity. So it was arranged with Microsoft that its Root Certificate Program, widely used throughout the Dutch public sector, would not yet revoke Diginotar's root CA status.[53]

The mitigation measures lacked a basis in law, even though the government acted in a public law dimension. Evidently, a government deciding to take over operations at a private company, without a legal basis, is highly controversial. The Minister justified the controversial approach emphasising the importance of the digital economy and the worldwide implication of DigiNotar trust revocation on the availability of and trust in (Dutch) online services. The confidentiality and integrity of communications was clearly of less importance to Dutch authorities. Apart from the delayed browser mitigation, this is also demonstrated by the fact as late as August 2012, Dutch tax advisors were still allowed to submit tax forms on behalf of clients to

[50] The amount of users that were impacted cannot be determined with certainty. ENISA 2011 observes: "the OCSP requests are only an indication, because not all browsers or clients make OSCP requests, and because OSCP requests could have been blocked or faked by attackers."

[51] ENISA 2011, p. 2.

[52] Fox-IT 2011, p.9. Around the time of the breach, millions of Dutch citizens submitted their income tax forms to the Dutch tax administration bureau, with 1 September as a deadline. It goes beyond the reach of this paper to fully research the implications of this fact, but it is a striking example of the amounts of sensitive information DigiNotar certificates were a crucial link in protecting. Still, in August 2012, tax advisors are using DigiNotar certificates for making submissions to the Dutch Tax office, see: http://www.rijksoverheid.nl/ministeries/fin/nieuws/2012/07/23/belastingdienst-waarschuwt-adviseurs-die-nog-gebruik-maken-van-diginotar-certificaten.html

[53] The relevant Parliamentary documents: *Kamerstukken II*, 26.643, 2011/12, numbers 188, 192, 194-210 and 214; *Handelingen II*, 2011/12, TK 102, nr 7 (question time); *Handelingen II* , 2011/12, nr 26 (DigiNotar).

the Dutch tax office using DigiNotar certificates.[54] We will return to these controversial mitigation measures in paragraph 4. The next section will explore security breaches at several other CA's to find returning vulnerabilities.

3.2 Multiple CA Breaches, History Repeating

Comodo – a CA that reportedly owns around one fifth or even quarter of the global SSL market – suffered several security breaches.[55] The foremost documented breach at Comodo was the compromise of its 'UTN-USERFirst-Hardware' certificate. According to data analysis from its SSL observatory, EFF calculated that '85,440 public HTTPS certificates were signed directly by UTN-USERFirst-Hardware. Indirectly, the certificate had delegated authority to a further 50 Certificate Authorities, collectively responsible for another 120,000 domains. In the event of a revocation, at least 85,000 websites would have to scramble to obtain new SSL certificates.'[56] Evidently, trust revocation would render all the HTTPS websites that use the certificates of this large CA untrustworthy, in effect leaving the websites inaccessible. The Electronic Frontier Foundation (EFF) describes this dilemma for browsers:[57]

> *'browsers would face a horrible choice: either blacklisting the CA quickly, causing outages at tens or hundreds of thousands of secure websites and email servers; or leave all of the world's HTTPS, POP and IMAP deployments vulnerable to the hackers for an extended period of time.'*

ENISA argued in the aftermath of the DigiNotar breach that if a larger CA would suffer a similar security breach, trust revocation by browser vendors in its certificates would seriously impact web communications on a global scale: 'it can even be argued that CA's of this size are too large to fail.'[58] Notably, EFF reports that the Comodo breach was discovered through smart cross-referencing of browser security updates by security researchers, rather than notification by the CA itself.[59]

VeriSign, another major CA, was hacked in 2010. The breach was only discovered by news agency Reuters in February 2012,[60] after Security and Exchange Commission regulations mandate companies to notify investors of intrusions since October 2011.[61] Apparently, administrators within VeriSign had kept the breach

[54] http://www.rijksoverheid.nl/ministeries/fin/nieuws/2012/07/23/belastingdienst-waarschuwt-adviseurs-die-nog-gebruik-maken-van-diginotar-certificaten.html

[55] See http://www.infosecurity-magazine.com/view/16986/comodo-admits-two-more-registration-authorities-hacked

[56] https://www.eff.org/deeplinks/2011/03/iranian-hackers-obtain-fraudulent-https

[57] https://www.eff.org/deeplinks/2011/03/iranian-hackers-obtain-fraudulent-https

[58] ENISA 2011, p. 2.

[59] Jacob Appelbaum and other security experts at TOR Project, whose account on the cross-referencing is highly recommended. See: https://blog.torproject.org/blog/detecting-certificate-authority-compromises-and-web-browser-collusion

[60] See: http://www.reuters.com/article/2012/02/02/us-hacking-verisign-idUSTRE8110Z820120202

[61] See: http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

silent, even for its top management. According to the Reuters reports, the former CTO Ken Silva claimed he had not learned of the intrusion until contacted by Reuters and said VeriSign 'probably can't draw an accurate assessment' of the damage, 'given the time elapsed since the attack and the vague language in the SEC filing'. VeriSign, meanwhile, claimed that 'there is no indication that the 2010 corporate network security breach […] was related to the acquired SSL product production systems.'[62]

From extensive public reporting on DigiNotar, we know that the CA had extremely poor security practises, which led to a landslide breach. The breach at CA GlobalSign is another example of poor security practises, as software running on a public-facing webserver was not updated. Information on the breach is limited, however, as the public only found out about the nature of this breach from an interview given by a company representative months after. From the interview, we learn that SSL operations weren't affected, because – unlike DigiNotar – GlobalSign had separated its critical infrastructure from its public-facing servers.[63]

From these cases, it emerges that users cannot inform themselves properly on the trustworthiness of certificates, even though legal documentation at CA's requires them to do so. As Vratonjic 2011 observes, users are confronted with information asymmetry.[64]

Technically, CA Trustwave did not suffer a breach. However, it became public that it had used its root CA status to enable third parties to issue arbitrary SSL server certificates (for employee monitoring purposes). Trustwave claims that this is common practice among other root CA's.[65] Regardless if this claim is true or false, it illustrates the compelled-CA attack of Soghoian & Stamm in real life:[66] CA's are in a unique position to enable surveillance of end-users.

This section has not covered all publicly known breaches.[67] Nonetheless, a pattern of vulnerabilities emerges. These systematic vulnerabilities will be discussed in the following section.

3.3 Systemic Vulnerabilities of the HTTPS Authentication Process

Many systemic vulnerabilities to the HTTPS ecosystem have already been observed in existing expert literature. These theoretical vulnerabilities have proven to be very realistic in recent years, primarily through the breaches described in the previous sections. Others are new in the sense that they emerge in the aftermath of these breaches.

[62] See http://www.reuters.com/article/2012/02/02/us-hacking-verisign-idUSTRE8110Z820120202

[63] See: http://www.zdnet.com/blog/btl/unpatched-server-led-to-globalsign-breach/75374

[64] Vratonjic 2011, p. 31.

[65] See: http://www.computerworld.com/s/article/9224082/Trustwave_admits_issuing_man_in_the_middle_digital_certificate_Mozilla_debates_punishment

[66] Soghoian & Stamm 2010.

[67] Roosa & Schultze 2010, p. 5 report on other breaches. Furhtermore, KPN/Getronics, StartSSL and several other CA's have been breached in recent years.

‘Systemic vulnerabilities’ point towards those vulnerabilities that are inherent to the HTTPS ecosystem as opposed to incidental vulnerabilities that have occurred at a particular stakeholder during an isolated incident. For instance, the fact that DigiNotar employed one extremely weak password to secure all of its systems is not a systemic vulnerability, but the fact that the result of poor security practises at one marginal CA’s may undermine the security of the entire HTTPS ecosystem is.

The fact that any CA can vouch for any domain name is probably the most important and widely recognised vulnerability. This makes each of the hundreds of CA’s in over fifty jurisdictions a single point of failure for potentially all HTTPS communications. Nobody knows the amount of CA’s and if a name is known, it is hard to tell what activities they employ.[68] This problem is augmented by the strong market incentives of root CA’s to organise subordinate CA’s or even sell their root status and default trust with browsers, by the relative ease of setting up your own CA and buying yourself into a chain of trust. The scenario’s for failure are manifold: any CA could facilitate or be a malicious actor engaging in cybercrime, or be a company monitoring its employees, or could be compelled by a state actor to enable mass surveillance of internet users,[69] or one of its administrators could simply have a bad day – forgetting updates, writing poor code or in his own right be coerced to cooperate in malicious activities. As ENISA observes: ‘The security of HTTPS equates to the security of the weakest CA.’[70]

The weakest CA known to date, DigiNotar, even passed the periodic audits, both the ones based on Dutch regulation for qualified certificate issuers and those based on internationally recognised industry standards. As successful audits negotiate CA root status by web browsers, all major browsers trusted DigiNotar by default – irrespective of its poor security standards. The perceived security that the current auditing schemes should deliver is another systemic vulnerability of HTTPS.[71]

The recurring information asymmetries are another striking systemic vulnerability. Organisations – including CA’s and websites – have strong incentives to conceal poor security practises and breaches. The reputational damage can be harmful, especially when trust is a selling point. If we look at CA’s, that have structurally failed to inform both browsers and the public about breaches, a breach risks not only the untrustworthiness of the entire ecosystem, but also renders trust of end-users unjustified: end-users may disclose highly sensitive information based on erroneous assumptions of security. This may be even more harmful than no HTTPS protection at all. Looking at websites, information asymmetries also occur. Proper HTTPS employment and implementation are seldom, since websites have strong incentives no to do so (see para. 2.2), but it is impossible for a user to tell how websites have implemented HTTPS. In light of these information asymmetries, the average user cannot be expected to evaluate the security practises of both CA’s and websites, even though HTTPS communications are primarily in their interest and users bear the consequences, as soon as sensitive information is either intercepted or altered.

[68] Roosa & Schultze 2010, p. 5.

[69] Soghoian & Stamm 2010.

[70] ENISA 2011, p. 2.

[71] Roosa & Schultze 2010, p. 3.

From the viewpoint of browsers, the interests of providing connectivity versus assuring trustworthiness may conflict. This is demonstrated in the overruling of OCSP responses and in browser management of root status. If a major CA is breached or trust in a widely used certificate is revoked, the damage from a communications security perspective may be all the more alarming, but browsers face the hard choice of rendering a large part of the HTTPS encrypted web inaccessible to its end-users. If ENISA notes that major CA's are too big to fail, big CA's being a single point of failure is even more worrying. Marlinspike convincingly stresses that browsers (and end-users) are locked-in to the operations of (major) CA's, and points towards a lack of 'trust agility' in the HTTPS ecosystem: on the one hand, a major CA cannot be untrusted at any moment, on the other, end-users hardly have control over where to base their trust.[72] Moreover, the damage associated with security breaches is pushed downstream by the value chain stakeholders and lies with end-users, even though end-users cannot reasonably be held accountable to evaluate security practises in the current HTTPS authentication model.

These systemic vulnerabilities illustrate a deeper problem in the current ecosystem, namely that the incentives structure of the HTTPS value chain leads to bad security. Websites want certificates as cheap as possible, CA's want to sell as many as possible, and browsers may prioritise connectivity and usability over security (as in the case of overruling negative OSCP responses). The current institutional incentive structure in the HTTPS ecosystem has caused a race to the bottom in terms of communications security. Moreover, in the current ecosystem, users cannot meaningfully influence security decisions and are faced with information asymmetries and liability transfer on their part. Our institutional analysis echoes what many security experts had been warning for, namely that the current HTTPS trust model is fundamentally flawed.

One of the classic functions of regulation is to structure market complexities, such as sub-optimal incentive structures in light of certain public interests. The next paragraph will delve into the role of regulation in solving the systematic vulnerabilities of the HTTPS ecosystem.

4. Governance

So far, we have described the thriving market for HTTPS and argued that its current structure comes with a set of theoretical systemic vulnerabilities in terms of communications security, that have proved to be quite realistic with a host of breaches.

Currently, the HTTPS trust model is by and large unregulated in both the US and the EU.[73] Over the last months, several (self-)regulatory initiatives are popping

[72] As discussed in para. 2.2. Moxie Marlinspike, 'SSL And The Future Of Authenticity', Presentation at the BlackHat USA 2011 conference.

[73] N. van Eijk, DigiNotar: Lessons to be learnt, Ars Aequi, 2012-2, p. 80-82. M.B. Voulon, 'Toezicht op certification service providers (CSPs)', Computerrecht 2012/1. Roosa & Schultze 2010. Industry standards are formulated, amongst others, by the American Bar

up around the globe, in particular a series of self-regulatory guidelines by a new industry entity, the CA/Browser Forum, and a very recent proposal by the European Commission – the 'eSignatures Regulation'.[74] The latter has taken the form of a Regulation, and thus has direct effect in all EU member states once adopted at the EU level. It contains several paradigm shifts when it comes to HTTPS governance that, if enacted in its current form, will impact the HTTPS ecosystem globally.

This paragraph sets out to stress the importance of identifying the values underlying HTTPS governance, before balancing various interests that are at stake in the HTTPS ecosystem. In paragraph 4.2, we return to our central research question, and examine if, and if so, how pressing systemic vulnerabilities that are inherent to the HTTPS value chain should be resolved through regulation. Here, an EU perspective is adopted in order to come to a concrete policy examination regarding the current EU initiative.

4.1 Values Underlying HTTPS Governance

One informative area of scholarship in the field of information security is of quite recent date.[75] Security economics posits that security fails when organizations or users that defend the systems lack an incentive to do so. Through its incentive-based analysis, security economics has explained various persistent security failures throughout the electronic communications environment with the use of economic concepts, such as information asymmetries, externalities and liability dumping. Over the last decade, it has influenced scholarship and policy in the field of information security significantly.

We have argued that several systemic vulnerabilities are inherent to the current constellation of incentives within the HTTPS value chain. As such, this parper has been inspired by security economics. The natural reflex in instances of sub-optimal market outcomes, or what in economic scholarship on HTTPS has been referred to as market failure,[76] is to call for regulation in the public interest.

Clearly, the security of the HTTPS ecosystem has a public interest dimension. Throughout the paper, we have seen many private and public interests enter the fray. But, as in security economics scholarship, we have largely related our description of the systemic vulnerabilities of the HTTPS ecosystem to the concept of (information) security, more specifically secure electronic communications – without seeking to conceptualise the underlying values of information security any further.

Before one can start to identify and balance private and public interests, however, the both essential and complex endeavour for governance, is to develop a deeper understanding of the values underlying regulatory intervention. As Feintuck observes: 'the establishment of a coherent structure of context-specific substantive

Association, the American Institute of Certified Public Accountants, the CA/Browser Forum and ETSI.

[74] See: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/558

[75] A good overview is given in T. Moore, R. Anderson, 2011. Internet Security. In: Peitz, M., Waldfogel, J. (Eds.), The Oxford Handbook of the Digital Economy, Oxford University Press. See: ftp://ftp.deas.harvard.edu/techreports/tr-03-11.pdf

[76] Vratonjic 2011.

values and principles is a necessary prior task to effective regulation in pursuit of public interest objectives.'[77] These substantive values are fundamentally derived from the *constitutional* values of legal systems. Mirroring the core of the cultural, social and economic fabric of a legal system, constitutional concepts come closest to a longer term consensus on how governance should structure society. These values underlying HTTPS governance – that, first and foremost, are shaped within constitutional contexts – need to be made explicit to achieve regulatory legitimacy.[78] It is only hereafter, that one can start questioning which specific regulatory measures constitute legitimate regulatory interventions in the HTTPS ecosystem.

Across jurisdictions, there seems to be consensus on the triad that information security seeks to protect: the *confidentiality*, *integrity* and *availability* of information.[79] In other words: 'the protection of information and information systems against unauthorised access or modification of information, whether in storage, processing, or transit, and against denial of service to authorised users.'[80] Information security thus contains both a constraining and enabling dimension. Constraining the access of unauthorised users to this trusted communications channel between two end-points (information source and end-users) on the one hand, while enabling a service between these authorised end-points on the other. This resonates with the aim of HTTPS communications, which is to seek an authentication handshake (constraining communication to authorised end-points) and set up an encrypted tunnel (enabling communication between the end-points).

Connecting the triad of confidentiality, integrity and availability to well-established constitutional values, two core constitutional rights emerge: i) privacy and in particular communications secrecy and ii) freedom of communication. These rights are prominently enshrined in the most influential constitutions around the globe, including the International Covenant on Civil and Political Rights ('CCPR', resp. art. 19 and art. 17[2]), the US Constitution (resp. First and Fourth Amendment), the European Convention on Human Rights ('ECHR', resp. art. 8 and art. 10). With regard to EU legislation, the recently adopted Charter of Fundamental Rights of the European Union incorporates the levels of protection provided in the ECHR in art. 52[3] and prescribes that EU regulation needs to respect its rights and principles according to art. 51[1] of the Charter.

The scope and weight given to these constitutional values varies across jurisdictions as they mirror the fabric of society, as mentioned before. Given the global distribution of the HTTPS ecosystem and its actors, it doesn't surprise that the weight given to various values underlying HTTPS governance may differ from one local constitutional setting to another. This complicates, or may even render impossible, global consensus on legitimate HTTPS governance. It is beyond the scope

[77] Feintuck 2010, The Oxford Handbook of Regulation (eds. M. Lodge, M. Cave & R. Baldwin),Oxford University Press: Oxford 2011, p. 42. See: http://www.oxfordhandbooks.com/oso/private/content/oho_business/9780199560219/p014.html#oxfordhb-9780199560219-chapter-3

[78] Idem, p. 56.

[79] K. de Leeuw & J. Bergstra (eds.), The History of Information Security: A Comprehensive Handbook, Elsevier: Amsterdam 2007, p. 2/3. ISO/IEC 27000:2009, para. 2.19. The 2002 Federal Information Security Act, 44 U.S.C. para. 3542.

[80] K. de Leeuw & J. Bergstra 2007, p.2.

of this contribution to provide an exhaustive conceptualisation of the HTTPS ecosystem against local deviations of these well-recognised constitutional values.[81] Nonetheless, some general remarks can be made on basic requirements that legitimate HTTPS governance should consider against the background of aforementioned constitutional texts.

The CCPR comes closest to a consensus on constitutional values, as the convention is generally ratified by a host of nations including the United States and all EU member states.[82] In the convention, the concept of 'correspondence' in Article 17 CCPR (art. 8 ECHR likewise) does include the integrity and confidentiality of electronic communications such as provided by HTTPS.[83] In the United States, the protection of privacy under the Fourth Amendment has for long been related to the 'reasonable expectations' users may have in a given context. ECHR jurisprudence has been inspired by this criterion. This is an important notion for HTTPS governance. If users have reasonable expectation of the protection HTTPS aims to provide, constitutional frameworks across (Western) societies grant these users strong privacy safeguards.

While perhaps less obvious, all three dimensions of information security critically relate to the freedom of communication. Art. 10 ECHR, the First Amendment and art. 17[2] CCPR protect the entire process of communications, not merely the content of expressive conduct.[84] Consider political speech and the DigiNotar affair: the man-in-the-middle interception of communications by Iranian authorities appears to have been targeted on activists, who placed unjustified trust in the end-to-end encrypted confidential communications HTTPS should have provided with dire – some experts argue even lethal – consequences.[85] The relation between HTTPS security and both freedom of expression and communications secrecy is no abstract matter.

As for both rights, they are considered enablers of other constitutional values, such as the freedom of association and religion, which renders them of considerable importance. Apart from refraining to interfere with these rights, state parties may have a positive obligation to effectively ensure their enjoyment through legislation.[86] The UN has explicitly recognized that protection of confidentiality and integrity the extends to cases in which information dissemination systems are operated by private firms.[87] Local deviations to these notions notwithstanding,

[81] Comprehensive information provided by L. Asscher, Communicatiegrondrechten: een onderzoek naar de constitutionele bescherming van het recht op vrijheid van meningsuiting en het communicatiegeheim in de informatiesamenleving, Amsterdam: Otto Cramwinckel Uitgever, 2002 (with English summary).

[82] For a full list of nations that have either signed or ratified the CCPR, visit: http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=en

[83] CCPR art. 17, General Comment 16/32, §8. In depth: M. Nowak, 'Privacy: Art. 17 CCPR', p. 403, in: M. Nowak, 'U.N. Covenant on Civil and Political Rights: CCPR commentary', Kehl am Rhein: Engel 1998

[84] Asscher 2002.

[85] See paragraph 3.2.

[86] CCPR/G/GC/34, §11.

[87] General Comment 16/32, §3-§4; Nowak supra note 9, p. 401.

regulatory interventions or exercises of executive power need to apprise the strong relation of the confidentiality, integrity and availability of secure web communications with the aforementioned constitutional parameters.[88]

Apart from constitutional values, HTTPS is instrumental to a range of other public and private interests – if implemented properly. HTTPS facilitates user trust in E-Commerce solutions, authenticates legal businesses and safeguards financial transactions. It should make life harder for cybercriminals, thus contributing to user trust and protection and lowering cybercrime levels. Governments may be able to cut financial expenditure on public administration, while democratic participation thrives in sufficiently secured communications environments.

These are just some of the many interests involved in the proper functioning of secure communications. In light of confidentiality, integrity and availability, these interests may directly lead to confrontations of these three underlying values of information security. CA trust revocation by browsers is a striking example: trust revocation renders many websites inaccessible (‘availability’), while maintaining an insecure status quo increases vulnerability to eavesdropping (‘confidentiality’) or alteration of transmitted information (‘integrity’) substantially.

The act of balancing confidentiality, integrity and availability keeping the manifold of interests in HTTPS communications in mind is, ultimately, a normative and policymaking exercise. Views on the exact manifestation of HTTPS governance will vary from one legal and political system to the other. But underlying constitutional values – notably privacy, communications secrecy and freedom of expression – provide minimum safeguards for end-users in HTTPS governance. And on a general level, any exercise of governmental power, if it be through regulatory intervention or executive action, requires justification and a basis in law.[89] If these constitutional values are not observed, HTTPS governance will fall short on legitimacy. As we will see, this is what happened in the aftermath of the DigiNotar affair.

4.2 The EU proposal for an eSignatures Regulation

In June 2012, the European Commission proposed a Regulation on ‘electronic identification and trust service for electronic transactions in the internal market’.[90] This section discusses several of the pressing vulnerabilities of the HTTPS ecosystem on a theme-by-theme basis, in the context of the EU proposal. In the conclusion, we abstract from the EU proposal to offer general remarks on HTTPS governance that should be useful to European policymakers and regulators as well as in other regions.

The proposed Regulation will replace the 1999 Electronic Signatures Directive discussed in paragraph 3.2. The ordinary legislative procedure will be

[88] A recently formulated constitutional value in the EU Charter is ‘the freedom to conduct a business’ in art. 16. Recent European Court of Justice case-law indicates that the relation with other rights still has to materialize. See A.M. Arnbak, case note Brein v. Ziggo & XS4ALL, AMI, 2012-3, p. 119-131.

[89] G. Lautenbach, ‘The Rule of Law Concept’, Amsterdam Faculty of Law Ph.D. Thesis, Jan. 2012, p. 2 & p. 231.

[90] European Commission, COM(2012) 238/2.

followed, meaning that the definitive contents of the Regulation are to be negotiated between the Council and European Parliament. Once enacted, a Regulation acquires the status of binding legislation in all EU Member States.[91] The following themes are discussed: A) Underlying Values; B) Scope; C) Liability; D) Security Requirements; E) Security Breach Notification, and F) Supervision.

A) Underlying Values

As discussed in paragraph 4.1, for regulation to achieve legitimacy, its underlying values need to be made explicit and need to be connected with constitutional values. Indeed, the recitals and the explanatory memorandum of the EU proposal illuminate that it aims to facilitate the digital economy. Other values mentioned are instrumental to economic development, but do not seem to be a policy goal of the EU proposal in itself. Building user trust, creating a single EU market and the rise of cybercrime, are seen as either 'key' or 'major obstacles' to the digital economy.[92] Furthering economic interests is connected to the constitutional value of creating a single market within the EU and finds its basis in articles that are referred to in the proposal, namely art. 114 (and art. 26) of the Treaty on the Functioning of the European Union ('TFEU').

Facilitating other constitutional values is required by the EU Charter, but is not formulated as an aim of the proposal. Constitutional values such as privacy, communications secrecy and freedom of expression are of paramount relevance in the context of website authentication. Related to this, is the omission in the EU proposal of a coherent vision on what information security should seek to protect. We have elaborated on the triad of availability, confidentiality and integrity of communications and shown how these may conflict. The EU proposal does not provide explicit guidance on how to balance these interests. Given the economic rationale of the EU proposal, the availability of communications is seemingly prioritised. Confidentiality and integrity are merely mentioned in the context of the legal fact that the Data Protection Directive (95/46/EC) applies for trust service providers (art. 11). Freedom of expression goes unmentioned in the EU proposal.

The priority given to economic interests and the lack of a coherent vision how to balance economic and constitutional values may have several concrete consequences for policy. As we will see, the EU proposal grants the European Commission and supervisory bodies executive power with regard to several of its important themes. This may come in the form of delegated acts for the Commission (fx. regarding security practises, art. 15[5]) and/or binding instructions for supervisory bodies (fx. security breach notifications, art. 15[4]). When formulating these delegated instances of exectuve power, and looking for guidance at the EU proposal, European and national institutions might feel obliged to follow the economic rationale over the broader interests that involve information security and constitutional values.

[91] Cf. art. 288 TFEU.

[92] European Commission, COM(2012) 238/2, recitals 1-4. The Impact Assessment also places strong emphasis on the Digital Single Market and economic interests. SWD(2012) 135, p. 34-39.

B) Scope

Art. 2[1] of the EU proposal established that the Regulation applies to 'trust service providers established in the Union' and not to the 'provision of electronic trust services based on voluntary agreements under private law'. The accompanying Impact Assessment mentions that 'at this stage, it is hard to define specific clauses for website authentication'.[93] Consequently, the EU proposal does not aim to alter the current data flows in HTTPS authentication through regulation.

The impact of the EU proposal on HTTPS communications may seem limited. However, several of its general provisions – on liability, supervision, security breach notifications, security practises, etc. – will impact the ecosystem in an unprecedented way as these are targeted at 'trust service providers'.[94] These 'trust service providers' include natural or legal persons that are involved in website authentication, i.e. CA's issuing SSL certificates.[95] The fact that the EU proposal 'establishes a legal framework for […] website authentication' can be regarded as a paradigm shift, now that the HTTPS ecosystem is still by and large unregulated, at least in the EU. We will discuss these general provisions later on. Next to the 'trust service providers', the EU proposal contains the characterisation of 'qualified trust service providers'. As in the 1999 Directive, the issuers of 'qualified' trust services face a stricter regulatory regime on supervision (art. 16), initiation requirements (art. 17) and certificate requirements (art. 19), amongst others.

Apart from the CA's, other critical stakeholders in the Actor Based HTTPS Authentication Value Chain – browsers and websites – remain unregulated. The Impact Assessment hints at 'an obligation for legal person's website to include trusted information (e.g. a certificate) allowing the user to verify the authenticity of the website and the existence of the legal person' and continues explaining the advantages of such an obligation. However, the EU proposal opts not to regulate this issue and leave it to the HTTPS market. The argumentation in the official documentation falls short in many respects. The Impact Assessment vaguely mentions 'commercial practises of browsers', without explaining the dynamics, and complains that 'specific rules are hard to define', without any further explanation of the perceived complexity. It even argues against such an obligation, because 'not all EU organisations are securing their website' – which obviously is an exceptionally poor argument.[96] But the Impact Assessment leaves the option open for Commission and Member States to 'play a role in ensuring such information' in the future.

The HTTPS value chain between information providers and customers is thus not reflected in the proposed EU regulatory framework. As to trust service providers, only those established in the EU are covered (art. 2[2]).[97] This runs the

[93] European Commission, SWD(2012) 135, p. 88.

[94] Art. 3[7] sub 14 & sub 15.

[95] Art. 3[7] sub 12 explicitly refers to 'website authentication', while the Impact Assessment details that this refers to the issuance of SSL certificates: European Commission, SWD(2012) 135, p. 86-88.

[96] European Commission, SWD(2012) 135, p. 35 & p. 87.

[97] Art. 10 contains provisions on qualified trust service providers from third countries (outside the EU), who should be accepted as such in the EU if a similar level of security, data protection and supervision is warranted in such an agreement.

risk of not addressing some essential vulnerabilities of the HTTPS ecosystem and placing a disproportionate amount of burden on a specific part of a subset of the value chain, namely European CA's.

C) Liability

Currently, liability for security breaches is disclaimed across the HTTPS value chain. The risks and damages of breaches are transferred to end-users, even though end-users cannot be reasonably held accountable to evaluate security practises in the current HTTPS authentication model.[98] In art. 9[1], the EU proposal introduces a new liability regime for 'trust service providers'. The exact wording of the provisions reads:[99]

> *'A trust service provider shall be liable for any direct damage caused to any natural or legal person due to failure to comply with the obligations laid down in Article 15(1), unless the trust service provider can prove that he has not acted negligently.'*

The explanatory memorandum has only a short sentence on the meaning of art. 9. It provides for 'entitlement to compensation of damage caused by any negligent trust service provider for failure to comply with security good practices which result in a security breach which has a significant impact on the service.'[100] Article 15[1] contains a new obligation on security practises (discussed under D).

The official documentation lacks any argumentation for introducing the new liability regime for CA's. The potential influence of the CA breaches is not made explicit in the proposal nor in its accompanying documents. But earlier responses of the European Commission to parliamentary questions raised in the aftermath of the DigiNotar breach,[101] ENISA policy documents[102] and lobbying by the Dutch government[103] suggests that the DigiNotar affair has made its mark in the drafting process, perhaps reflected in this liability provision.

The breaches at CA's are indeed a concern to HTTPS communications and point to substantial negative externalities associated with a breach at one isolated CA, as the entire HTTPS ecosystem is at risk of being compromised. A liability regime may incentivise (European) CA's to take security more seriously. In addition, the last sentence of art. 9[1] places the burden of proof with the CA and may lead to investment in proper logging functions. And root CA's might become more cautious to sell their root status to subordinate/intermediate CA's.

On the other hand, introducing liability regimes for European CA's may have several perverse effects. CA's are mostly unaware of the type of certificate they

[98] See paragraph 3.3.

[99] Article 9[1].

[100] European Commission, COM(2012) 238/2, p. 6.

[101] See: http://www.europarl.europa.eu/sides/getDoc.do?type=WQ&reference=E-2011-007985&language=EN

[102] ENISA 2011.

[103] Ministry of Internal Affairs letter to the Dutch Parliament, 'diginotar onderzoeken', kenmerk 2012-0000150459, p. 3/4.

sell in a specific context, whereas website owners know what kinds of sensitive information they are dealing with. A liability regime might be favourable for incumbent CA's who are more able to insure themselves against substantial breaches. Small CA's will think twice before doing business with large corporations processing vast amounts of sensitive data, or might not even enter that market segment at all.

More fundamentally, the proposed liability regime doesn't appreciate the dynamics of the HTTPS authentication value chain. Art. 9 has two dimensions, one of which is not thought through in the proposal: 'negligence' and 'any direct damage'. Regardless of the security practises and intentions of one individual CA ('negligence'), no single company is able to stand in for the consequences of the entire HTTPS ecosystem ('any direct damage') once its systems are breached. As every CA is a single point of failure, a security breach enables false certification of HTTPS communications across the entire internet. Consider DigiNotar: an annual budget of a few million US Dollars, whereas certificates were issued for activities of Google, Facebook, Skype, cia.gov, etc. (see para. 3.2). In such a scenario, liability for any given (European) CA not only seems unreasonable, but outright harmful. No single company is able to stand for the direct damage of such potential value.

HTTPS value chain analysis suggests alternative approaches, in which liability is spread across the value chain according to the risk associated with certain activities. CA's have their share in this risk, but so do certificate purchasing parties such as websites (online banking, E-Commerce, private communications, etc.) and even browsers, in the case of untimely trust revocation. Another aspect that would deserve attention in the context of liability, is the ability for CA's and other stakeholders to pass on liability to information technology producers such as software developers, who in many cases 'are in a better position than database owners to fix problems with information security'.[104]

The currently introduced liability regime may have a positive effect on security practises at CA's and mitigate liability transfers to end-users. But if liability arrangements are not spread throughout the value chain, it risks favouring incumbent CA's and placing a disproportionate amount of burden on CA's in general. This point needs to be addressed in the upcoming legislative procedure.

D) Security Requirements

The EU proposal introduces a second new obligation for CA's, on security requirements. CA's need to implement 'appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide [..] having regard to the state of the art', according to art. 15[1]. 'In particular, measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders of adverse effects of any incidents.' Compliance will be monitored by a supervisory body ex art. 13[2a] and failure to comply will cause the CA to be liable for any direct damages on the basis of art. 9[1].

The specific security requirements are not summed up in the Regulation. So much of the impact of the security requirements provision depends on the details.

[104] Winn 2009, p.33.

Both the Commission and national supervisory bodies are granted executive power to adopt delegated acts and issue binding instructions on the basis of art. 15[4] to 15[6]. The open-ended norms of art. 15[1] provide flexibility for regulators and enforcers to adapt security requirements in line with best practises. But with this flexibility at a delegated regulatory level, balancing of different interests and underlying constitutional values is equally important. Notably, recital 26 mentions that the security requirements should serve 'to boost user trust in the single market', rather than to protect the integrity and confidentiality of trust services. The recital seems to imply that security requirements are there to keep up appearances with users, rather than meaningfully contributing to securing HTTPS communications and the systems it relies on. As observed before, we see a prevailing economic rationale, rather than one concerned with the broader underlying interests of information security and constitutional values.

Apart from CA's, we have noted in paragraph 2.2 that HTTPS implementation at the most popular websites on the internet is below 10%, while proper implementation supporting 'the state of the art' protocol of HSTS (HTTP Strict Transport Security) is around 1%. Out of 185.000 of the most popular websites surveyed, only 13% has protected itself against the recent BEAST attack. While incentivising CA's to employ good security practises is important, a real challenge that is not addressed by this EU proposal lies with website HTTPS implementation. Once again, a value chain approach towards regulation would have exposed this important aspect of HTTPS security.

E) Security Breach Notification

With all CA breaches discussed in paragraph 3, the structural tendency is to (try and) keep it a secret for both browsers, websites, authorities and the public. Strong incentives exist to do so.

Security breach notifications ('SBN's') should, at least in theory, minimise the damage after a breach has occurred and provide incentives for organisations to invest in information security upfront. The EU proposal introduces such a breach in art. 15[2]. European CA's are to notify relevant authorities of a breach of security or a loss of integrity 'where feasible within 24 hours', if the breach 'has a significant impact on the trust service provided and on the personal data maintained therein'. If disclosure of the breach is in the public interest, relevant authorities may inform the public or require the CA to do so.

Cross-border breaches should be notified by the authorities to the relevant supervisory bodies in other Member States and to ENISA. Supervisory bodies are to report on the notifications to the European Commission and ENISA (art. 15[3]).

There appears to be broad consensus that SBN's are an appropriate measure to relieve the HTTPS ecosystem of perceived trust in an succeeded authentication, where the validity of the authentication is unwarranted.[105] It is telling that the security breach at VeriSign only became public two years after the incident and through an

[105] ENISA 2011, p. 3.

indirect way, when Security and Exchange Commission regulations mandated companies to notify investors of intrusions since October 2012.[106]

But SBN legislation is not a silver bullet in augmenting security levels. Much of their impact will, again, depend on the details of the SBN legislation, as experience with SBN legislation in the United States learns. The authority to formulate these details is, as with the security requirements provision, delegated. The European Commission may formulate implementing acts (art. 15[6]), that explicitly can include circumstances under which breaches should be notified, and supervisory bodies (art. 15[4]) may issue binding instructions. A notable task for the Commission is to determine in which circumstances breaches have a 'significant impact' on the service itself or the processed data. Furthermore, SBN's should be complemented with strong enforcement, in order to avoid non-compliance. If this fails to materialize, strong incentives exist not to notify breaches at all, at the expense of the well-intentioned companies that take security and the interests of customers seriously.[107] Another lesson from the US experience is to avoid 'safe harbors', instances in which companies are exempted from notification, for encrypted data. Winn notes that this creates 'perverse incentives to invest in mitigating harms after they occur instead of prevention'.[108]

F) Supervision

After quite careful consideration in the Impact Assessment, the European Commission has decided to leave the implementation of supervision structures to the Member States.[109] This is articulated in the general provision on supervision of art. 13. Supervision will remain confined along the lines of nation states. Art. 14 mandates mutual assistance between supervisory bodies in the different Member States.

Art. 13[1] establishes that the bodies 'shall be given all supervisory and investigatory powers that are necessary for the exercise of their tasks'. These tasks are summed up in art. 13[2a], and include supervision over 'trust service providers' with regard to the security requirements and SBN mandated by art. 15. The explanatory memorandum states that in this respect, the EU proposal clarifies and enlarges the role of supervision.[110] The Impact Assessment gives some normative guidance on supervision: 'SSL Certificates providers will be supervised in a transparent and neutral manner'.[111] Transparency of supervisory activities is achieved through a reporting obligation (art. 13[3]), whereas the provision has no further wording on the 'neutrality' of the supervisor.

[106] See: http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

[107] J. Winn, Are "Better" Security Breach Notification Laws Possible?, 24 *Berkeley Tech. L.J.* 1133-65, 2009, p. 33.

[108] Winn 2009, p. 3. Similarly D. Thaw, Characterizing, Classifying, and Understanding Information Security Laws and Regulations, forthcoming Ph.D. dissertation, University of California, Berkeley, May 2011.

[109] European Commission, SWD(2012) 135, p. 40-42.

[110] European Commission, COM(2012) 238, p. 6.

[111] European Commission, SWD(2012) 135, p. 88.

In the Netherlands, the need for a legal basis for supervisory intervention has been illustrated in the aftermath of the DigiNotar affair. The mitigation and recovery by public authorities lacked a legal basis with regard to essential steps. As described in paragraph 3.1, the take-over of operational processes at a CA and negotiating with market parties with respect to trust revocation delay are both controversial exercises for the executive branch of government. The question rises, whether these interventions would have been legitimate under the EU proposal.

The EU proposal introduces a new legislative basis for supervisory activities with regard to security practices and SBN's in the HTTPS ecosystem. But the supervision provision seems to be overbroad and too narrow at the same time. The 'tasks' can only be broadened by amending the future Regulation, as art. 13[5] does not grant the Commission the authority to formulate new 'tasks'. Conversely, given the generous formulation of art. 13[1] – 'all supervisory and investigatory powers that are necessary' – the EU proposal hardly restricts the exercise of executive power in these fields. This distribution of power may be problematic in two respects: the flexibility regarding the exercise of executive power may be overbroad from the viewpoint of legitimacy, while the rigidity regarding the 'tasks' of art. 13[2] may be too narrow to include future possible tasks of a supervisory body that may be necessary to ensure adequate enforcement.

Returning to the DigiNotar breach, art. 13 and 15 don't provide for an operational takeover, as it falls outside of the scope of the tasks of supervisory bodies as defined in art. 13[2a], which merely authorises 'monitoring' of compliance, and issuing binding instructions as regulated through art. 15[4]. Negotiating trust revocation with browsers cannot fall under the latter, as these do not constitute trust service providers. In addition, the economical justification by Minister Donner that the availability of HTTPS communications had to be safeguarded, seems at risk with the communications security that art. 15 seeks to achieve – particularly considering the false certificates that were issued for some of the biggest websites on the internet.[112] So even though the audit services of the Dutch government hailed the mitigation of the DigiNotar breach by Dutch authorities ('the government has showed its teeth'[113]), the mitigation measures would lack a legal basis even under the current proposal.

On the basis of the EU proposal, a yearly audit is mandatory for qualified trust service providers (art. 16[1]) but not for trusted service providers, i.e. most CA's (art. 15[1]). Trust service providers *may* submit a report of a security audit to the supervisory body to confirm that is complies with the security requirements of art. 15[1]. The value of these audits is questionable, however. As mentioned in paragraph 3.3, the weakest CA known to date, DigiNotar, passed its annual ETSI audits for 'qualified' CA's mandated by Dutch law. If the aim is to incentivise CA's to comply with art. 15[1], well-crafted liability provisions may have more chance to warrant this than the perceived security auditing schemes may deliver.

[112] See paragraph 3.1.

[113] RAD/2012/161, 'De zaak 'DigiNotar': handelde de overheid adequaat?', 8 March 2012, p. 11.

5. Conclusion & Analysis: Regulating the HTTPS Value Chain

The CA collapse has been a long time coming. This paper shows that actor-based value chain analysis provides insight into the incentives structure of HTTPS stakeholders and helps to explain the alarming race to the bottom regarding the security of HTTPS communications. After several alarming breaches at CA's, recognition for the real and alarming security vulnerabilities that are inherent to the HTTPS authentication model is broadening. The DigiNotar affair has brought home that Internet security is no abstract matter and that violations can have serious consequences. Meanwhile, our dependence on HTTPS grows with the day.

The recent EU proposal to amend the existing regulation on electronic signatures contains some of the first regulatory explorations on HTTPS governance. Abstracting from our analysis of the proposed eSignatures Regulation, some general observations can be made regarding HTTPS governance.

First and foremost, the proposal targets a limited group of stakeholders in the HTTPS value chain, namely European CA's. As such, the proposed legal framework focuses on only one actor in the value chain. If the systemic vulnerabilities of HTTPS are to be addressed through regulation, governance should reflect on the incentives and interactions of its stakeholders throughout the entire HTTPS authentication value chain. Apart from CA's, what is the role of browsers, websites and end-users and how should one allocate responsibilities between them? CA's have their share in the systemic vulnerabilities of HTTPS, but so do websites that initiate HTTPS communications and process valuable information or facilitate transactions and browsers that play a pivotal role in trust revocation and root CA status verification.

To achieve legitimate HTTPS governance, the underlying values of HTTPS governance should be explored and expressed. In particular, the balancing of private and public interests should be connected to agreed constitutional values that provide baseline requirements for governance. If information security is an important value underlying a particular regulatory effort, or HTTPS governance in general, the concept should be untangled and a coherent vision should be developed on how to balance the triad of availability, confidentiality and integrity of information.[114] Furthermore, the exercise of executive power through delegated acts and supervisory arrangements needs a solid legal basis, as the DigiNotar mitigation illustrated. The EU proposal falls short in this respect, as it omits to conceptualise underlying values beyond the economic rationale. Privacy, communications secrecy and freedom of expression are hardly mentioned as rationales, even though the EU Charter mandates that these constitutional values are to be respected. This weakens the legitimacy of the EU proposal considerably.

The proposal targets CA's established in the European Union. By its very nature, the HTTPS ecosystem is a global techno-social ecosystem. The EU proposal and its accompanying official documentation seem to navigate past the complexities and tensions between a global ecosystem on the one hand, and the inherent locality of

[114] A nice example of such a conceptualization of information security can be found in Mulligan & Schneider 2011. On the basis of an exploration of its underlying values, the authors formulate a set of principles that should guide cybersecurity policy.

a EU proposal on the other. Is ‘territorial law evasion’[115] a risk in the value chain? Or does the proposal alter the incentive structure of websites, in the sense that EU established CA’s become more attractive as opposed to those based in, say, the US? This leads to the question, if approximation of laws between jurisdictions is justified, even though constitutional values may differ.

Returning to the systemic vulnerabilities of HTTPS communications, the fact that any CA can vouch for any domain name is probably the most important and widely recognised vulnerability. This makes each of the hundreds of CA’s in over fifty jurisdictions a single point of failure for potentially all HTTPS communications. Regulation can play a very limited role in altering such inherent design choices in HTTPS authentication, given the slow speed of the regulatory cycle and its inherent locality, amongst others.[116] Furthermore, it runs the risk of reinforcing systemic vulnerabilities as it may create new long-term institutional dependencies on the actors whose roles should be limited from a security perspective, such as CA’s.

Lately, technical solutions have been suggested to address specific aspects of this systemic vulnerability. Google’s ‘CA pinning’ proposal seems promising, because it lets browsers only accept certificates for a domain name issued by a CA chosen by the domain holder, instead of any of the hundreds of CA’s around.[117] Being a company of considerable size and active as a browser and web service, it can leverage such systemic changes throughout the value chain in the short term.

HTTPS governance may play a role in creating the right incentives for critical actors in the HTTPS value chain on the short-term. So apart from CA’s, policy reflection is needed on the desirability of mandating websites to employ certain security practises (type of certificate, state of the art implementation, CA pinning) where private communications are offered, sensitive data is processed or financial transaction are facilitated. Browsers could be mandated to scale up the impact of trust revocation and root CA verification. On the short term, specific measures to be considered throughout the value chain may include proportional liability provisions, realistic security breach notifications and security requirements, but much will depend on the details of these provisions. Careful consideration must be given to the impact of these measures on the incentive structures in the HTTPS ecosystem. In any event, legitimate HTTPS governance apprises the incentive structure of the entire HTTPS authentication value chain and connects its balancing of public and private interests to underlying values, and in particular constitutional rights such as privacy, communications secrecy and freedom of expression. In the long term, a robust technical and policy overhaul must address the systemic weaknesses of HTTPS, as each CA is a single point of failure for the security of the entire ecosystem.

[115] J. Feick & R. Werle 2010, ‘Regulation of Cyberspace’ in: *The Oxford Handbook of Regulation*, p. 542.

[116] Idem.

[117] ENISA 2011, p. 3. More information: http://www.imperialviolet.org/2011/05/04/pinning.html