Do you "TRUST" me?

Author: Bill Corbitt
http://www.linkedin.com/in/bulwarkz

Abstract:
This paper analyzes several recent breaches of major players in the security industry, in particular security products vendors and Certificate Authorities (CAs). Distinct patterns and relationships have emerged that have allowed the prediction of the next set of potential targets. Without the implementation of stringent compliance standards for CAs one can expect that governments will intervene with the only outcome being a global impact to the freedom of trade.

Note to the Reader:

The research included in this paper does not address the circumstances around how the Certificate Authorities (CAs) were breached nor how their Rogue Certificates were issued. What is questioned is "Trust" – Trust with the CAs and their ability to maintain a high level of security within their industry.

The Certificate Authority (CA) [1]:

A certificate authority, or CA, holds a trusted position because the certificate that it issues binds the identity of a person or business to the public and private keys (asymmetric cryptography) that are used to secure most Internet transactions.

When a business or person wants to use these technologies, they apply to a Certification Authority. The CA collects information about the person or business that it will certify. Depending on the intended use and level of security required, certain rules are followed, called "certificate policies".

These rules may make it necessary to verify the applicant's information before issuing the certificate. For example, when a business wants to offer products for sale on a secure web site, the CA will usually check to make sure that the applicant really has responsibility for the domain.

However, this particular policy wouldn't apply to someone who just wants to encrypt his or her personal e-mail.

The processes that use the public key, such as a web browser, check the certificate to make sure that it comes from a trusted CA and may also check to be sure that the information is consistent with the way that it's being used. All major web browsers "trust" a series of CAs and have packaged them in the 'web of trust' for each browser's store.

Digital certificates would typically be issued from a CA, i.e., Entrust.com, Thawte, or other CAs that vouches for the authenticity of their public keys. (There are over 500 CAs.)

Overall, a digital certificate from a trusted CA is like getting a passport, or government identification card. Someone like a Notary Public, the CA, verifies that you are who you say you are. Each CA is unique because each CA has its own CA Public Key that is used to determine the CA's own identity.

Background:

With several CAs reporting breaches, compromised or rogue certificates have emerged, as have clear trends and patterns that tie breaches of certain CAs together.

[1] http://www.rsa.com/glossary/default.asp?id=1010

Subsequent links of trust between the CAs display a sobering commonality. Further modeling also provides grounds to anticipate potential breaches or the issuance of rogue certificates with certain CAs.

Consideration was given to the type, amount and proliferation of network security breaches of the CAs. Relevancy was also given to the issuance of rogue certificates and in one instance a possible private key compromise[2].

Attention has been given to the business relationships between the CAs that have been targeted, and the timing of the attacks. How the breaches occurred is not relevant to this discussion.

Chronology:[3]
The pattern between the compromised CAs that has been reviewed focuses on CAs with one or several of the following in common: breached networks, rogue or compromised certificates, or a compromised private key.

A chronological timeline of the breached CAs will be discussed first. With this timeline details that are relevant to the actual event. Lastly, we will note the relationships to the compromised CA or RA and their relationships with DigiNotar and Symantec CAs.

Digicert (Malaysia): 17-Sep-07
Digicert Sdn Bhd Malaysia is an intermediate certificate authority that was certified by parent authority *Entrust*. Digicert Sdn Bhd Malaysia issued poorly encrypted certificates that were compromised because of technical and procedural weaknesses in the certificate generation process.

> "There is no indication that any certificates were issued fraudulently, however, these weak keys have allowed some of the certificates to be compromised,"[4]

*Per the Entrust Bulletin, Digicert Sdn Bhd Malaysia should **not** to be confused with Digicert (US-based CA)[5] Digicert US (Utah) and Digicert Sdn Bhd Malaysia are different companies.*

The exposure of Digicert to the DigiNotar compromised certificates has not appeared on their web site revocation list[6]. This could be due to the fact that DigiNotar is in bankruptcy protection and no longer issuing CAs.

Kaspersky: 8-Feb-09
Kaspersky seems to be a popular target. Identified by at least three different sources (The Register, eWeek & Softpedia) Kaspersky has sustained three attacks 2008, 2009 and 2010.

The Kaspersky breaches have been selected mainly because the initial exploits of the DigiNotar started with simple web defacements that have a similar profile to the Kaspersky incidents.

> *(2009) A security lapse at Kaspersky has exposed a wealth of proprietary information about the anti-virus provider's products and customers, according to a blogger, who posted screen shots and other details that appeared to substantiate the claims.*[7]
>
> *It hasn't been smooth sailing for security vendor Kaspersky Labs over the last few years. Back in 2008, the company's Malaysian website was defaced by a Turkish hacker via an SQL injection. In 2009, their U.S. support*

[2] *Private Keys make the Public Key that is used to determine the CA's own identity.*
[3] Refer to Appendix K

[4] http://www.theregister.co.uk/2011/11/03/certificate_authority_banished/
[5] http://www.entrust.net/advisories/malaysia.htm
[6] http://www.digicert.com.my/_support/02_crl.htm
[7] http://www.theregister.co.uk/2009/02/08/kaspersky_compromise_report/

site was compromised -- again by the use of an SQL injection.[8]

(2010) Hackers have caused serious embarrassment for a major security technology company. Kaspersky Lab's Website was hacked over the weekend, sending customers looking for security software to an external download page pushing counterfeit software.[9]

Russian antivirus vendor Kaspersky Lab has confirmed the unauthorized online availability of its intellectual property in the form of source code ... In a statement sent to Softpedia, the company says that partial source code for its 2008 range of consumer products was stolen almost three years ago by a former employee.[10]

Comodo (AddTrust External): 15-Mar-11
On March 15th 2011, a Comodo affiliate RA was compromised resulting in the fraudulent issue of 9 SSL certificates spread across 7 unique domains. At no time were any Comodo root keys, intermediate CAs or secure hardware compromised.[11]

Note: Review the Comodo (AddTrust External) trust relationship to DigiNotar compromised certificates (Appendix F).

Here is where a "Trust" trend is starting to develop. This "Trust" is with the breached CA DigiNotar.

The "Comodo Hack"[12] is a key component of the CA breaches. Interesting enough that Comodo officially announced another (unnamed) affiliate CA breach.

> Another Registration Authority, or RA, that resells digital certificates for Comodo was compromised, in addition to the original RA breached a week ago, Comodo founder Melih Abdulhayohlu told CNET today. He would not name the company but said it was located in Europe and was attacked over the weekend.[13]

RSA: 17-Mar-11
Despite no trust relationship between Comodo and RSA, the compromise of the SecurID™ two-factor Authentication methodology has caused concern among most security professionals.

It is widely considered that two-factor authentication is believed to be stronger protection than passwords alone and is therefore required by law, industry standards and best practices for authenticating access to critical applications/systems and highly sensitive data.

Announcements relevant to both the Comodo affiliate RA breach and the RSA breach are similar. Both companies allude to the complexity of their breaches.

StartCom/StartSSL: 15-Jun-11
StartSSL has suspended issuance of digital certificates and related services following a security breach on 15 June. A trademark of Eddy Nigg's StartCom, the StartSSL certificate authority is well known for offering free domain validated SSL certificates, but also sells organization and extended validation certificates.[14]

[8] http://downloadsquad.switched.com/2010/10/20/kaspersky-has-its-own-security-breached-yet-again/
[9] http://www.eweek.com/c/a/Security/Kasperskys-Download-Site-Hacked-Directs-Users-to-Fake-AntiVirus-336193/
[10] http://news.softpedia.com/news/Kaspersky-Confirms-Source-Code-Leak-Threatens-Legal-Action-Against-Downloaders-181456.shtml
[11] http://blogs.comodo.com/it-security/data-security/the-recent-ra-compromise/
[12] http://blogs.comodo.com/it-security/data-security/the-recent-ra-compromise/
[13] http://news.cnet.com/8301-27080_3-20048831-245.html
[14] http://news.netcraft.com/archives/2011/06/22/startssl-suspends-services-after-security-breach.html

DigiNotar/(PKIoverheid)[15]: 19-Jul-11
"DigiNotar"[16], the Dutch CA who is now filing for bankruptcy because of their breach by the "ComodoHacker"[17] and has a direct relationship with not only Symantec CAs, but most of the other major CAs that have announced breaches.

Review of the list of compromised DigiNotar certificates, DigiNotar Damage Disclosure[18], shows a relationship with major CAs and sub-CAs discussed herein.

Note: PKIoverheid (PKIGovernment), the government 'leg' of DigiNotar, has not announced a breach but they have revoked their digital certifications. Both Chrome and Firefox have banned both CAs for life[19].

Symantec Breach: 7-Sep-11
The Symantec breach[20] should be given careful consideration. Remember that the breach actually occurred in 2006 not in 2011 when it was formally announced. Symantec is not only a security product vendor but Symantec also owns, and operates, several Certificate Authorities. Among these are VeriSign, RapidSSL, Thawte, and GeoTrust.

(DigiNotar/Thawte): 7-Sep-11
The quickly retracted statement from the Dutch Government, that Thawte was also breached is of serious concern.

> *Then, yesterday a Dutch government agency erroneously made a statement that Thawte had been breached. Although the statement was proven false and quickly retracted, it highlights the fear and knee-jerk reactive actions proliferating as a result[21].*

Subsequently, this brings into question why the Dutch Government would retract such a precise comment. There are three general scenarios;

> **One:** When governments are faced with a common enemy of 'the state', they often ally themselves with other governments in an extension of 'good will' and cooperation.
>
> **Two**: The Dutch government honestly believed that Thawte was breached.
>
> **Three:** The Dutch government misinterpreted some information and reacted prematurely.

This behavior from any government is notable and should be taken seriously.

Note: Appendix D shows a trust relationship with a large number of compromised DigiNotar certificates and Thawte.

GlobalSign: 15-Jun-11
Certificate authority GlobalSign admitted it suffered a web server attack but did not find any evidence of rogue certificates being issued, compromised certificates, or exposed customer data. The security firm stopped issuing SSL certificates from September 5th–15th after the company discovered that it had been attacked.[22]

[15] http://www.vasco.com/company/press_room/news_archive/2011/news_diginotar_reports_security_incident.aspx
[16] http://www.darkreading.com/authentication/167901072/security/attacks-breaches/231600498/digital-certificate-authority-hacked-dozens-of-phony-digital-certificates-issued.html
[17] http://www.networkworld.com/news/2011/090611-comodo-hacker-claims-credit-for-250454.html
[18] https://blog.torproject.org/blog/diginotar-damage-disclosure
[19] http://www.theregister.co.uk/2011/09/03/diginotar_game_over/
[20] http://www.eweek.com/c/a/Security/Symantec-Confirms-Source-Code-Stolen-in-2006-Breach-It-Didnt-Know-About-690167/
[21] http://www.symantec.com/connect/blogs/diginotar-ssl-breach-update
[22] http://www.zdnet.com/blog/btl/globalsign-breach-confirmed-ssl-certificates-not-compromised/65328

GlobalSign also has a noted trust relationship with DigiNotar (Appendix H). So far, of all the trusted CAs to DigiNotar we have three breaches that all have the trusted relationship with the compromised DigiNotar Certificates.

*GlobalSign has **not** announced a compromise.*

Note: Appendix H shows a trust relationship between GlobalSign and the compromised DigiNotar certificates.

KPN: 7-Nov-11
The largest telecommunications company in the Netherlands has stopped issuing SSL (Secure Sockets Layer) certificates after finding indications that the website used for purchasing the certificates may have been hacked.

The backend infrastructure used to generate certificates does not appear to have been affected, although an investigation is under way with results expected soon, KPN spokeswoman Simona Petescu said on Monday.[23]

KPN announced this week that it has suspended issuing certificates after discovering the breach of a PKI-related Web server with a distributed denial-of-service tool that apparently had been sitting on the server for at least four years.[24]

Gemnet[25]**:** 8-Dec-2011
Hackers apparently penetrated the Gemnet's websites and their databases were accessed.

KPN moved to allay fears that the hack would lead to the creation of false certificates. The company said that no systems related to the certificates themselves had been compromised in the attack and the Dutch PKIoverheid key infrastructure was not in any danger. The incident is the high-profile breach to hit a Dutch certificate authority this year and the second breach at a KPN form. In November, a server breach at KPN Corporate Market forced the company to temporarily close its site.[26]

Note: KPN was breached on 7-Nov-11 and now an "affiliate" of KPN is breached on 8-Dec-2011.

VeriSign: 2-Feb-12
According to an article by Joseph Menn on Reuters, VeriSign Inc. was repeatedly hacked in 2010. The details can be found in the U.S. Securities and Exchange Commission filing in October 2011, when VeriSign said that in 2010,

"... the Company faced several successful attacks against its corporate network in which access was gained to information on a small portion of our computers and servers. We have investigated and do not believe these attacks breached the servers that support our Domain Name System ("DNS") network."[27]

These attacks happened in 2010. This would place the timeframe of the actual attack **between** the Kaspersky **and** the Comodo attack but **after** the Symantec breach.

Note: *Symantec acquired VeriSign in 2010.* Appendix C shows a trust relationship between VeriSign and the compromised DigiNotar certificates.

Peculiarity of Breaches:

DigiNotar gets breached and its parent company is Vasco Data Security International Inc. (Vasco).

[23] http://www.infoworld.com/d/security/kpn-stops-issuing-ssl-certificates-after-possible-breach-178250
[24] http://www.darkreading.com/authentication/167901072/security/attacks-breaches/231902517/certificate-authority-uncovers-old-breach.html
[25] http://www.theregister.co.uk/2011/12/08/certificate_authority_hacked/
[26] http://www.darknet.org/?p=893
[27] http://www.bitdefender.com/blog/VeriSign-Breach-May-Shatter-Enterprise-Trust-42.html

Vasco is a maker of the Digipass, a two-factor token[28] that is a direct competitor of the RSA SecurID product.

RSA and Vasco sell other authentication products. For example, Vasco sells a CAP (Cardholder Activated PIN entry device) that enables chip cards (credit or debit) to be used as an authentication mechanism. Vasco Data Security International Inc. (Vasco)[29], has a 70% market share[30] in the 'Two-Factor' authentication market in Europe.

Vasco's key digital CA (DigiNotar) gets breached and on 17 March 2011 while the two-factor business of RSA also suffered a breach. The similarity between the two companies is worth noting.

Evaluation of the relevancy pertaining to the CA compromises and their "relationships" with the TAAs needs to be considered. Simply, as an industry, we would be reckless not to challenge these relationships and the security architectures of both the CAs and the Token Authentication Authorities (TAAs).

Note: The CA subsidiary of Vasco (DigiNotar) has announced a breach; no facts exist for concluding that the token activities of Vasco have been compromised.

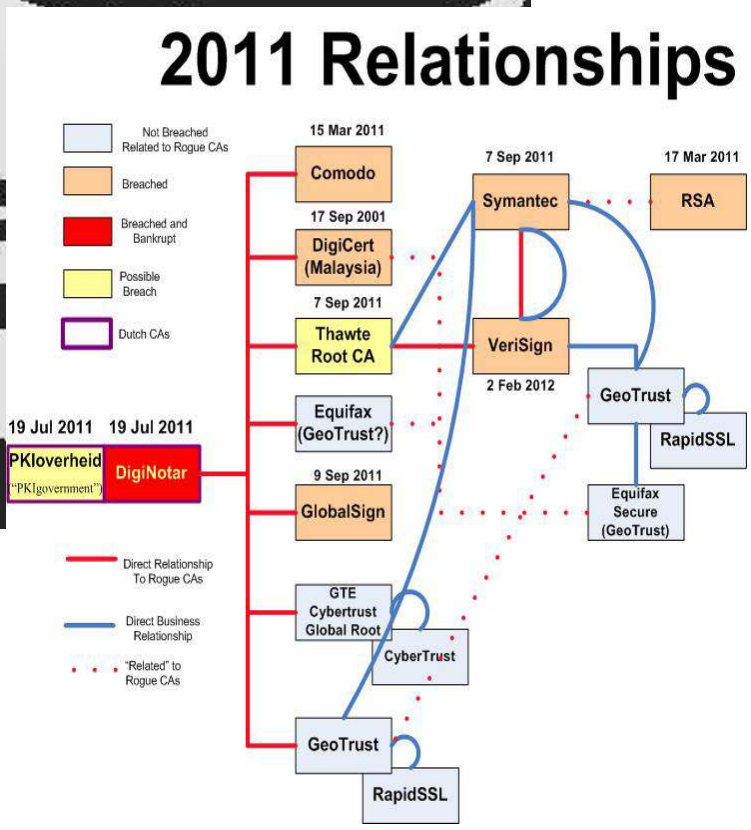
Comment: Similarly, while RSA acknowledged a break of their two factor business, no available information enable us to conclude that their CA activity was also breached.

There is a need to challenge those CAs who trusted the CAs of DigiNotar. After all shouldn't they, as part of business due diligence, validate their security?

> DigiNotar eventually went bankrupt after an investigation revealed that shoddy security led to the issuance of dozens of counterfeit credentials, including one for Google Mail that was used to target more than 300,000 people accessing their Gmail accounts. [31]

Relationships and "Trust":

The relationships and breaches among each of the CAs diagramed in Appendix I (see insert) is interesting. In this diagram the breaches associated with the "trust" of DigiNotar but also the associated CA compromises or "Rogue" CAs starts to come to light.

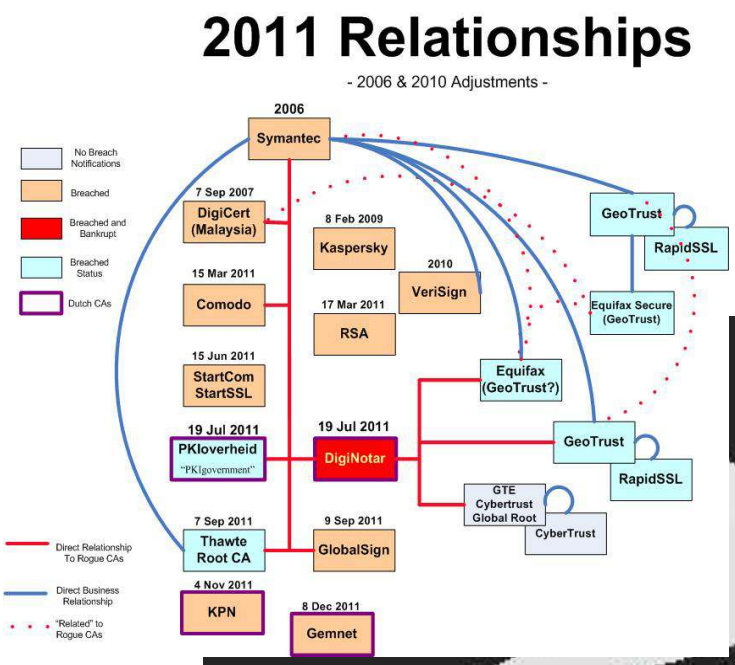


[29] http://www.theregister.co.uk/2011/08/29/fraudulent_google_ssl_certificate/

[30] http://digipass.net/investor_relations/financial_reports/financial_reports.aspx

[31] http://www.theregister.co.uk/2011/12/08/certificate_authority_hacked/

When you consider the "adjusted" breach timelines in Appendix J (see insert) you have a significantly different perspective on what could actually be occurring between the CAs.



The commonality of the dates, the entities breached, the business and CA trust relationships all display a clear "Trust" relationship between these CAs.

Note: Additional CAs could also have suffered a compromise that remains undetected or undisclosed to date.

CA Proliferation:
There is a disturbing correlation between the sequence of targeting the CAs and their ranking according to CA Proliferation, or "Size".

A presentation from the SSL Observatory, Peter Eckersley and Jesse Burns (*USENIX Security 2011*), may have unwittingly identified the "*target base*" for the next set of attacks. They ranked the CAs according to proliferation[32].

Top Roots by CA Proliferation[33]

1. Deutsche Telekom Root
   a. 252 sub-CAs
   b. 4,164 leaves
2. CyberTrust Global Root
   a. 93 sub-CAs
   b. 20, 937 leaves
3. AddTrust External CA Root* (Note below)
   a. 72 sub-CAs
   b. 384, 481 leaves
4. GlobalSign Root CA *(Private Key rumored to be compromised)*
   a. 63 sub-CAs
   b. 140, 176 leaves
5. Entrust.net Secure Server Certification Authority
   a. 33 sub-CAs
   b. 91, 203 leaves
6. ValiCert Class 3 Policy Validation Authority
   a. 20 sub-CAs
   b. 1,273 leaves
7. VeriSign, Inc, Class 3 Public Primary Certification Authority
   a. 18 sub-CAs
   b. 312, 627 leaves

***Note:** "AddTrust External CA" could be Comodo.*

Comodo[34]
CN = AddTrust External CA Root
CN = AAA Certificate Services
CN = COMODO Certification Authority

Comment: With Digicert (Utah) there has been a "Trust" with a set of compromised DigiNotar Certificates (Appendix G).

From the list of Top Roots by CA Proliferation 3 of the 7 "Top Roots" (GlobalSign, VeriSign, AddTrust External – *Comodo*) have officially announced breaches. Of the aforementioned three only one, GlobalSign, may have possibly had their private keys compromised.

[32] http://static.usenix.org/events/sec11/tech/slides/eckersley.pdf
[33] http://static.usenix.org/events/sec11/tech/slides/eckersley.pdf
[34] http://www.safemashups.com/royaltyfree.html

Guilt by Association:

Based on the facts presented in this review there are compelling reasons to assume that the Symantec CAs are in "*Breached Status*".

One area not discussed until now is the potential use of pcAnywhere by the Symantec engineers. Symantec engineers could have used the remote access software (pcAnywhere) throughout the Symantec environment from 2006 – after the initial breach – until present day.

Their engineers would have utilized the company's own software as a matter of standard business practice – any company would have done the same thing.

In the event Symantec would have discontinued the use of their compromised [35] pcAnywhere software internally and subsequently this would have translated to its prolific use.

Facts to consider;

1) "Zero day" vulnerabilities in the pcAnywhere source code that was compromised[36],
2) The announcement by the Dutch government that Thawte was also breached, and its immediate withdrawal,
3) The delayed announcement of the Symantec and VeriSign breach's, and
4) Exposure of the Symantec CAs to the "Rogue" DigiNotar Certificates, and
5) The combined breaches of Symantec and VeriSign.

List of Symantec CAs that are considered to be in a "*Breached Status*" are as follows;

1) Thawte
2) GeoTrust
3) Equifax (GeoTrust)
4) RapidSSL

Targeting:

Considering all the relationship models discussed (Appendix I & J), the "Rogue" CAs from the DigiNotar breach (Appendix B – H) and the information from the Eckersley and Burns presentation, a risk model can be constructed.

HIGH Risk of Future Compromise

1) CyberTrust Global Root[37]
2) GlobalSign
3) ValiCert Class 3 Policy Validation Authority
4) Entrust.net Secure Server Certification Authority
5) Deutsche Telekom Root

Comment: *"Compromise" includes network breach, compromised certificates, Rogue Certificates and exposure of the private key to malicious use.*

End of Innocence:

With over 500 or so CAs could they all have such shoddy security? There is nothing confirming that the CAs do not have "shoddy security".

With such shoddy security, which was noted in the Dutch Government"s posting of the DigiNotar breach [38], could be systemic in some of our most trusted facilities.

[35] http://www.cbsnews.com/8301-501465_162-57373518-501465/hackers-release-symantec-pcanywhere-source-code/

[36] http://www.cbsnews.com/8301-501465_162-57373518-501465/hackers-release-symantec-pcanywhere-source-code/

[37] Review Appendix J

[38] http://www.theregister.co.uk/2011/12/08/certificate_authority_hacked/

Currently, there is no auditable industry security standard for CAs. There is also no compliance standard or governance from which the general public can determine the security or compliance status of accredited CAs.

A catastrophic network breach or the issuance of "rogue" CAs in the near term, from other CAs, is of great concern.

> *Roel Schouwenberg, a senior security researcher with Kaspersky Lab, is advising internet users to exercise extreme caution when dealing with online certificates in the wake of the DigiNotar certificate authority (CA) systems hack. "We are still talking about 500 or so CAs out there," he explained on a conference call with analysts and researchers this week, noting that the DigiNotar CA hack was industrial espionage that has the potential to have the same effect on the industry as the Stuxnet malware.*[39]

Remediation Plan:
The CA industry must have a regulatory and compliance standard that assesses the security or integrity of the CAs. For anyone to assume that the CAs have an inherently secure environment is naïve at best. The industry must create a certification program that would be mandated to all publicly accessible CAs.

From his article, *Tenuous Chains Of Trust In Digital Certificates*[40], Mike Fratto outlines some obvious conclusions.

> "… because there is an inordinate amount of trust in all things SSL/TLS and the Golden Lock. (*Don't get me going on that farce called Extended Validation Certificates.)* The SSL/TLS protocol and the public key cryptography that underpins it are, as far as I know, well designed and trustworthy. Barring software vulnerabilities and poorly designed SSL/TLS libraries, such as the Python SSL library's default implicit trust of certificates that Brian Keefer points out in Unauthenticated SSL Sends a Dangerous Message, we can trust the protocol and the math."[41]

So if we can trust both the protocol and math where did we go wrong? Trust. The trust with CAs to protect their critical environments according to industry security standards cannot be assumed.

Compliance and Validation:
Trust validation can be conducted in the form of an auditable ISO security standard (for example under the umbrella of the ISO), or by a consortium between the major browser players and ISPs that would be similar to the approach taken in the financial sector by the Payment Card Industry Security Standards Council.

There is a compelling need for stringent security standards for all CAs/RAs. This also needs to be confirmed with a public validation and compliance process that is enforceable and auditable.

Recommendations:

1. Consider avoiding any "Trust" of the DigiNotar or Symantec CAs.

2. Most CAs[42] could have experienced, or are about to experience a catastrophic network breach, issuance of rogue certificates, compromise of existing certificates

[39] http://www.infosecurity-magazine.com/view/20770/kaspersky-senior-researcher-predicts-further-diginotarstyle-hacks-/
[40] http://www.networkcomputing.com/data-protection/229401024
[41] http://www.networkcomputing.com/data-protection/229401024
[42] VeriSign, ValiCert, Thawte, GeoTrust, RapidSSL, CyberTrust (Root Authority), DegiCert, Equifax and GeoTrust

or a key compromise in the near term.

3. The 5 CAs identified, as High Risk of Compromise should immediately consider conducting an intensive security evaluation.

4. Trust relationships with the TAAs (i.e., RSA, Vasco, etc.) should **NOT** be implicitly trusted.

5. Compromise of more CAs is a probability and any certificate should be carefully scrutinized before accepting trust.

6. The entire CA industry must undergo an end-to-end security compliance and evaluation program from which corporate decision makers should be held professionally accountable.

7. Those CAs identified, as being at "HIGH Risk" of breach should undergo a complete internal audit and security validation by a third party and make those results public.

8. Stricter standards for the complexity and strength of any issued certificates should be mandated.

9. Currently under laws such as California SB1386, companies are only required to disclose the breach of customer data, but not other data breaches. Any and all breaches of security for any CA/TAA should be made immediately available to the public.

10. An industry evaluation and compliance security certification program, through non-CA affiliated third parties, should be immediately instituted.

Conclusion:

Our trust in the CAs is in jeopardy.

The survey of 174 IT and IT security pros had several red flags about digital certificate management. Some 72 percent of organizations don't have an automated process in place in case their CA is hacked, so they can't automatically replace digital certificates. The risk there, of course, is a website or application outage in the event of an expired certificate.

Many (46 percent) can't even generate a report on digital certificates that are about to expire; it's a manual process to track certs that are reaching their expiration date.

"The survey confirmed our suspicions" based on what we've seen out there, says Jeff Hudson, CEO of Venafi. "People don't know what the hell's going on out there [with their certificates]." [43] (*Emphasis Added*)

The "TRUST" that business and governments have in these models can no longer be assumed to be safe and secure and must be validated.

Inevitable conclusion is the creation of rigorous set of security and compliance standards and certifications for all CAs.

[43] http://www.darkreading.com/authentication/167901072/security/news/232601373/survey-post-it-notes-spreadsheets-used-to-manage-digital-certificates.html?cid=nl_DR_daily_2012-02-27_html&elq=b4267d7829f94f64ae953f850b76cc7e

Credits

About the Author

Bill Corbitt has over 20 years of military and commercial computer security, investigative and computer forensic experience. Bill has experience in breach analytics, post-mortem breach analysis as well as risk impact determinations for Fortune 500 companies. As a former Federal Agent he was Program Security Officer (SAF/AQ) for advanced weapon systems and focused beam technologies.

Contributing Editors:

Al Stern experience ranges from building start-ups to strategy for Global 50 corporations; previous Co-Director of the University of Minnesota Center for Economic Education, and Director of Breck School, and taught a summer program in economics at Oxford University; B.S. and M.A. degrees from the University of Minnesota in education and economics.
http://www.linkedin.com/pub/allen-stern/1/215/775

Todd Bell is an Executive IT Security Advisor at ConnectTech, LLC specializing in Cyber security for PCI, HIPAA, and SCADA systems
http://www.linkedin.com/in/toddbell

Jeff Tutton, M.Sc., CISSP, CISA, PCI-QSA, leads Intersec Worldwide's Enterprise Risk Management Group, President of Global Security & Compliance
http://www.linkedin.com/in/jefftutton

Appendix A
Breach Dates

Date Made Public	Name	NOTE	Comments
17-Sep-07	DigiCert (Malaysia)	Sub-CA	Mozilla & Microsoft Revoked all certs
8-Feb-09	Kaspersky	(CA)	
15-Mar-11	Comodo	Root CA	
17-Mar-11	RSA	Root CA	Token Auth & Libs
15-Jun-11	StartCom/StartSSL	Root CA	
19-Jul-11	DigiNotar	Root CA	Hackers Issued Certs
7-Sep-11	Thawte*	Root CA	Similar to Symantec
7-Sep-11	Symantec pcAnywhere		2006 Breach?
9-Sep-11	GlobalSign	Root CA	ComodoHacker Claims he is holding the private key
7-Nov-11	KPN	Sub-CA	
2-Feb-12	VeriSign Inc.	Root CA	

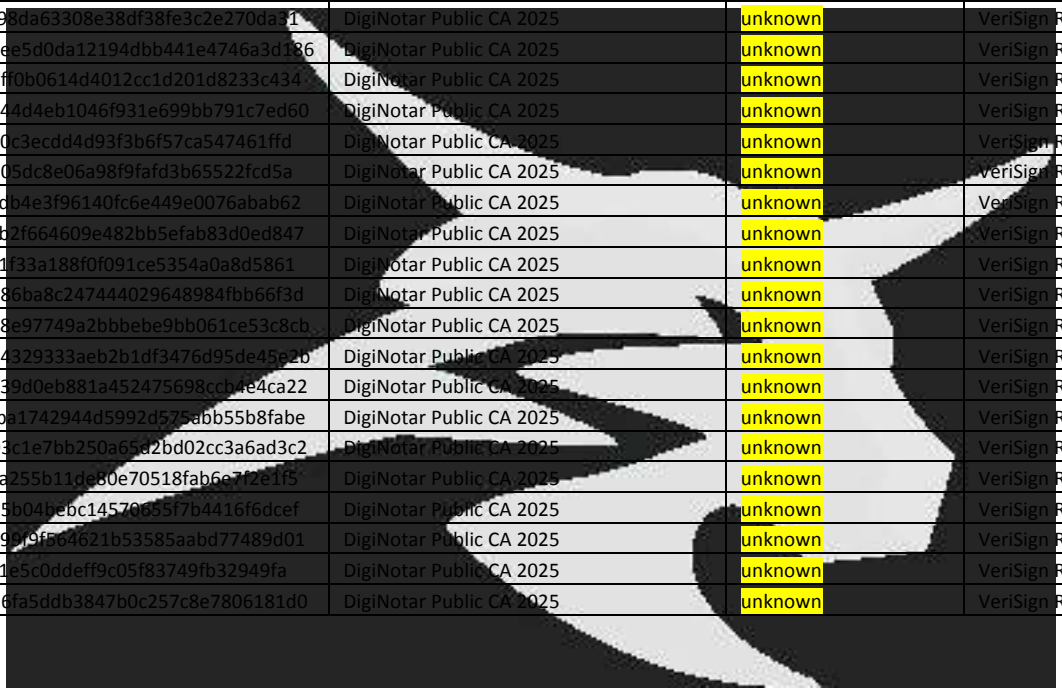
**Dutch Government Announced Breach Not Symantec*

Appendix B
DigiNotar / CyberTrust

cert md5	ca	revoked	cn
fd2e074189200dc3331da2c6d88d16d2	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:21:11.000	*.*.com
c9606aa0c22b4d697d65e930407f8ab1	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:21:30.000	*.*.org
5adf10c320682a82eec40e2647a17ba9	DigiNotar Public CA 2025	unknown	www.cybertrust.com
faa4a4aaecd42f9004f081d2c6900ba2	DigiNotar Public CA 2025	unknown	CyberTrust Root CA
d64cae632be935a1cae88838daaeffd1	DigiNotar Public CA 2025	unknown	CyberTrust Root CA
d8789b4ea4694195674be5eda15f1454	DigiNotar Public CA 2025	unknown	CyberTrust Root CA
bcc1dd9ebc3fb1320f207df0eb1dc46f	DigiNotar Public CA 2025	unknown	CyberTrust Root CA
0d4dc3c7d9858e01b12e3d13b5e30723	DigiNotar Public CA 2025	unknown	CyberTrust Root CA
6b857e65e6aa2baeec59b377ceda3751	DigiNotar Public CA 2025	unknown	CyberTrust Root CA
5e48219be6329fd6ef8b59a23d80ee5c	DigiNotar Public CA 2025	unknown	CyberTrust Root CA
8ea06caeb34ea2d751647676fdb3b4e1	DigiNotar Public CA 2025	unknown	CyberTrust Root CA
5baafd9f65037a8cabdb91ef5fe11330	DigiNotar Public CA 2025	unknown	CyberTrust Root CA
87c6933111b16eb2868dc216ba6f9d08	DigiNotar Public CA 2025	unknown	CyberTrust Root CA
fd23736d393420c044a721bf7e45d26e	DigiNotar Public CA 2025	unknown	CyberTrust Root CA
e9d1e44f7a4521cc920a8f771fe53e2e	DigiNotar Public CA 2025	unknown	CyberTrust Root CA
db448dca5d5206b1b151fb394d26e4f2	DigiNotar Public CA 2025	unknown	CyberTrust Root CA
e404935374c35b698276670face8e6e6	DigiNotar Public CA 2025	unknown	CyberTrust Root CA
85254f75aa0cc998757c4bcee265398	DigiNotar Public CA 2025	unknown	CyberTrust Root CA
b5d408944fb08d3659690eb6169ec1d5	DigiNotar Public CA 2025	unknown	CyberTrust Root CA
eeecbd9ae35537e231ca46522d8d8744	DigiNotar Public CA 2025	unknown	CyberTrust Root CA
4c91ea67d92fca927888b11942201887	DigiNotar Public CA 2025	unknown	CyberTrust Root CA
58447191631270ed3fac9871c7026528	DigiNotar Public CA 2025	unknown	CyberTrust Root CA
864bd76d754cf6fb6a6bf860bec0075e	DigiNotar Public CA 2025	unknown	CyberTrust Root CA

Appendix C
DigiNotar / VeriSign

cert md5	ca	revoked	cn
a51abb82a9dcd87872045f1dbd2cf9bc	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:19:25.000	VeriSign Root CA
fd2e074189200dc3331da2c6d88d16d2	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:21:11.000	*.*.com
c9606aa0c22b4d697d65e930407f8ab1	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:21:30.000	*.*.org
c7c98da63308e38df38fe3c2e270da31	DigiNotar Public CA 2025	unknown	VeriSign Root CA
181ee5d0da12194dbb441e4746a3d186	DigiNotar Public CA 2025	unknown	VeriSign Root CA
5d7ff0b0614d4012cc1d201d8233c434	DigiNotar Public CA 2025	unknown	VeriSign Root CA
35644d4eb1046f931e699bb791c7ed60	DigiNotar Public CA 2025	unknown	VeriSign Root CA
eeb0c3ecdd4d93f3b6f57ca547461ffd	DigiNotar Public CA 2025	unknown	VeriSign Root CA
2d805dc8e06a98f9fafd3b65522fcd5a	DigiNotar Public CA 2025	unknown	VeriSign Root CA
86ccb4e3f96140fc6e449e0076abab62	DigiNotar Public CA 2025	unknown	VeriSign Root CA
c59b2f664609e482bb5efab83d0ed847	DigiNotar Public CA 2025	unknown	VeriSign Root CA
6c01f33a188f0f091ce5354a0a8d5861	DigiNotar Public CA 2025	unknown	VeriSign Root CA
de586ba8c247444029648984fbb66f3d	DigiNotar Public CA 2025	unknown	VeriSign Root CA
1908e97749a2bbbebe9bb061ce53c8cb	DigiNotar Public CA 2025	unknown	VeriSign Root CA
e0b4329333aeb2b1df3476d95de45e2b	DigiNotar Public CA 2025	unknown	VeriSign Root CA
33539d0eb881a452475698ccb4e4ca22	DigiNotar Public CA 2025	unknown	VeriSign Root CA
8feba1742944d5992d575abb55b8fabe	DigiNotar Public CA 2025	unknown	VeriSign Root CA
bb03c1e7bb250a65d2bd02cc3a6ad3c2	DigiNotar Public CA 2025	unknown	VeriSign Root CA
7cda255b11de80e70518fab6e7f2e1f5	DigiNotar Public CA 2025	unknown	VeriSign Root CA
53b5b04bebc14570655f7b4416f6dcef	DigiNotar Public CA 2025	unknown	VeriSign Root CA
257909f564621b53585aabd77489d01	DigiNotar Public CA 2025	unknown	VeriSign Root CA
c801e5c0ddeff9c05f83749fb32949fa	DigiNotar Public CA 2025	unknown	VeriSign Root CA
8bb6fa5ddb3847b0c257c8e7806181d0	DigiNotar Public CA 2025	unknown	VeriSign Root CA



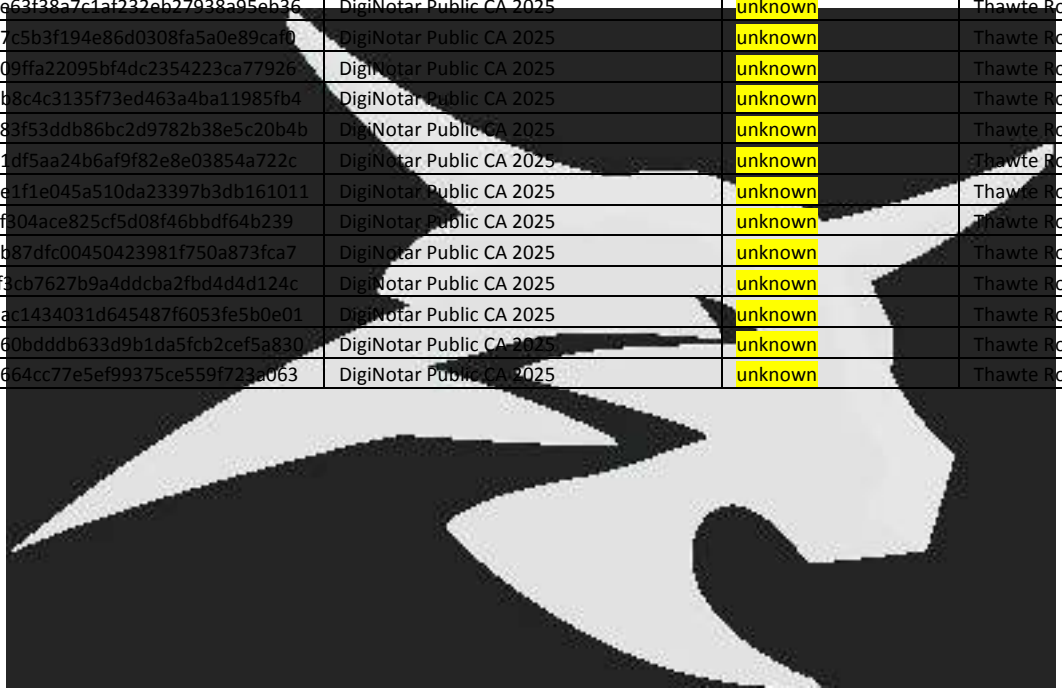
Appendix D
DigiNotar / Thawte Root CA

cert md5	ca	revoked	cn
846684390c34ce76b28643733c90496e	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:16:35.000	Thawte Root CA
7a7ce78fcb36609adf632260c925989a	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:17:47.000	Thawte Root CA
2a438a86fa7b6102f48e2b843f07558a	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:18:02.000	Thawte Root CA
9f8e980e8213ba994599bdbaced28e5d	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:18:17.000	Thawte Root CA
850cd3e8d3921b8b60a6787a8dd0c16c	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:19:09.000	Thawte Root CA
fd2e074189200dc3331da2c6d88d16d2	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:21:11.000	*.*.com
c9606aa0c22b4d697d65e930407f8ab1	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:21:30.000	*.*.org
73e2f21383d7ecdefe47a94a9f53f15a	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:21:39.000	Thawte Root CA
f1a0561b9ef54f6a717cbf4bfbf9f098	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:22:03.000	Thawte Root CA
dcb57a3c178f2ae40e951aef2f23d14d	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:22:15.000	Thawte Root CA
2cc12e8deb359d4b498bc193da072ea1	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:22:24.000	Thawte Root CA
fe688a86e3442e01ddc3cb4c9fe49ab1	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:01:04.000	Thawte Root CA
9059978508a5ec94f499a7437559034b	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 11:59:33.000	Thawte Root CA
3b7d88096fd435a93b1f8edaeb631b4f	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 11:57:40.000	Thawte Root CA
10bf40cc10464aa2f3203685d446e57e	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 11:58:48.000	Thawte Root CA
9426e2df5d7a4f32fdfde1ff44b955f1	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:00:21.000	Thawte Root CA
bf890f302ebde8ea6d429c0cb0f923ee	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:22:51.000	Thawte Root CA
25c61cb0afe45d4be802c5eb86d1aa71	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:03:51.000	Thawte Root CA
a07f55131f26de04cdf4db9ffda57cf2	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:23:00.000	Thawte Root CA
82a30c0cc7bc4db74ebd6693d2b7f8de	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:05:04.000	Thawte Root CA
294741f8e24c9d03815badd7f03b700c	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:23:10.000	Thawte Root CA
a359e3979ca60f7a975cb592e89f45ef	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:11:10.000	Thawte Root CA
5a9b26a0b310e08750e866f7cf971c5b	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:23:43.000	Thawte Root CA
cbc5c0d37d821546df611868acebc2a8	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:13:07.000	Thawte Root CA
eaad9f84ee58f1c59176036effc262ee	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:23:52.000	Thawte Root CA
1c72cccc2e5502d9aa083119ffc19df6	Koninklijke Notariele Beroepsorganisatie	2011-07-27	Thawte Root CA

	CA	12:16:47.000	
ef8d64da8e28dd26207a42bf0cba1a35	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:24:01.000	Thawte Root CA
f60abae05d7815884f3b5d39ac511609	DigiNotar Public CA 2025	unknown	Thawte Root CA
52c0d7aa8d35ba75dfbe3a99cb7b77bc	DigiNotar Public CA 2025	unknown	Thawte Root CA
6f1871d5268f2d3ec8733eb04f6f0dc4	DigiNotar Public CA 2025	unknown	Thawte Root CA

Appendix D
DigiNotar / Thawte Root CA

cert md5	ca	revoked	cn
726e1198628f89007525d0a007210db5	DigiNotar Public CA 2025	unknown	Thawte Root CA
54061c18bce2e8c0ea292c35c4be7c6b	DigiNotar Public CA 2025	unknown	Thawte Root CA
f33e34b34260ce14ae1c4cb41de0bf69	DigiNotar Public CA 2025	unknown	Thawte Root CA
b66187b1266b26518acc4a84be36f75e	DigiNotar Public CA 2025	unknown	Thawte Root CA
4a2e63f38a7c1af232eb27938a95eb36	DigiNotar Public CA 2025	unknown	Thawte Root CA
9647c5b3f194e86d0308fa5a0e89caf0	DigiNotar Public CA 2025	unknown	Thawte Root CA
9e409ffa22095bf4dc2354223ca77926	DigiNotar Public CA 2025	unknown	Thawte Root CA
b25b8c4c3135f73ed463a4ba11985fb4	DigiNotar Public CA 2025	unknown	Thawte Root CA
a1783f53ddb86bc2d9782b38e5c20b4b	DigiNotar Public CA 2025	unknown	Thawte Root CA
3541df5aa24b6af9f82e8e03854a722c	DigiNotar Public CA 2025	unknown	Thawte Root CA
168e1f1e045a510da23397b3db161011	DigiNotar Public CA 2025	unknown	Thawte Root CA
05af304ace825cf5d08f46bbdf64b239	DigiNotar Public CA 2025	unknown	Thawte Root CA
627b87dfc00450423981f750a873fca7	DigiNotar Public CA 2025	unknown	Thawte Root CA
f1df3cb7627b9a4ddcba2fbd4d4d124c	DigiNotar Public CA 2025	unknown	Thawte Root CA
06bac1434031d645487f6053fe5b0e01	DigiNotar Public CA 2025	unknown	Thawte Root CA
98660bdddb633d9b1da5fcb2cef5a830	DigiNotar Public CA 2025	unknown	Thawte Root CA
616664cc77e5ef99375ce559f723a063	DigiNotar Public CA 2025	unknown	Thawte Root CA

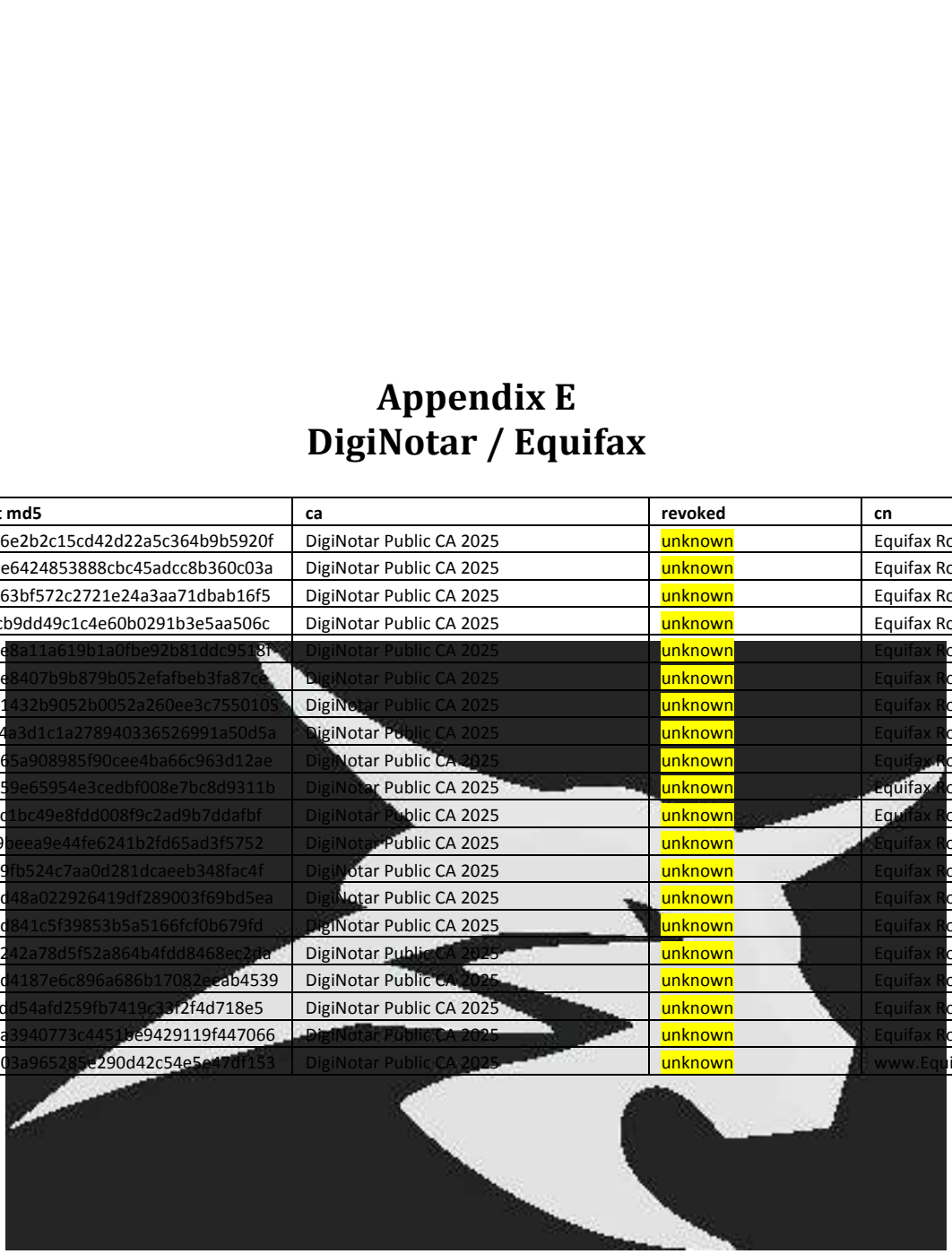


Appendix E
DigiNotar / Equifax

cert md5	ca	revoked	cn
fd2e074189200dc3331da2c6d88d16d2	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:21:11.000	*.*.com
c9606aa0c22b4d697d65e930407f8ab1	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:21:30.000	*.*.org
bfcb2fdbd765576b3c2bc44e025bfa96	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:17:36.000	Equifax Root CA
5a9c1cb8128c94a32da07d424e1fafd6	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:27:34.000	Equifax Root CA
9c0f7f2a3b2ccdb6c5f45c9e3c892fb8	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:18:54.000	Equifax Root CA
0274677ca738e8c58b2215b847f7ce00	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:25:24.000	Equifax Root CA
034e8aae08eed1ac1596a307f54933f3	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:20:21.000	Equifax Root CA
83e2d51c0e852cc4e787c946c6f4fdd3	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:25:32.000	Equifax Root CA
871edad93dc7a8a8af2dce437cbc169f	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:21:53.000	Equifax Root CA
01619b4e3cddd553d140081a014d7291	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:25:41.000	Equifax Root CA
b811c5bfd2f9b8ad5c1bb334d4480be5	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:22:42.000	Equifax Root CA
38d89ddcc743561570002a233b03b4f7	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:26:01.000	Equifax Root CA
a94f5f27694b035c02dfd4f459094ce4	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:23:33.000	Equifax Root CA
f331a23b07a1d6baf2cd3e80ea55fc5f	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:26:12.000	Equifax Root CA
a358cec55aa2eeb8aaece6d261317cb6	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:26:22.000	Equifax Root CA
6fbabf76393aa483e20c23c80ebe3677	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:25:15.000	Equifax Root CA
1754d164c21f974d649cc1d0fd1e2bdc	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:26:38.000	Equifax Root CA
0d5977f95f71b3690722da557e7e8b14	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:25:51.000	Equifax Root CA
c79c623a2e9bf505af315b87f7f7b917	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:26:48.000	Equifax Root CA
ad4d8b3d2d114d307dc66d63372813b8	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:26:58.000	Equifax Root CA
7f7561a37bd49a3f3818fdf2ebfb2e19	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:27:09.000	Equifax Root CA
cdc9e67e2ca0cba21d89ddb11dc520c0	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:27:20.000	Equifax Root CA
a78a2cf0080165855736b93ddc3f5397	DigiNotar Public CA 2025	unknown	Equifax Root CA

Appendix E
DigiNotar / Equifax

cert md5	ca	revoked	cn
2406e2b2c15cd42d22a5c364b9b5920f	DigiNotar Public CA 2025	unknown	Equifax Root CA
47be6424853888cbc45adcc8b360c03a	DigiNotar Public CA 2025	unknown	Equifax Root CA
1e063bf572c2721e24a3aa71dbab16f5	DigiNotar Public CA 2025	unknown	Equifax Root CA
bfccb9dd49c1c4e60b0291b3e5aa506c	DigiNotar Public CA 2025	unknown	Equifax Root CA
627e8a11a619b1a0fbe92b81ddc9518f	DigiNotar Public CA 2025	unknown	Equifax Root CA
454e8407b9b879b052efafbeb3fa87ce	DigiNotar Public CA 2025	unknown	Equifax Root CA
1e81432b9052b0052a260ee3c7550105	DigiNotar Public CA 2025	unknown	Equifax Root CA
72c4a3d1c1a278940336526991a50d5a	DigiNotar Public CA 2025	unknown	Equifax Root CA
90065a908985f90cee4ba66c963d12ae	DigiNotar Public CA 2025	unknown	Equifax Root CA
05559e65954e3cedbf008e7bc8d9311b	DigiNotar Public CA 2025	unknown	Equifax Root CA
6a5c1bc49e8fdd008f9c2ad9b7ddafbf	DigiNotar Public CA 2025	unknown	Equifax Root CA
cf59beea9e44fe6241b2fd65ad3f5752	DigiNotar Public CA 2025	unknown	Equifax Root CA
1e79fb524c7aa0d281dcaeeb348fac4f	DigiNotar Public CA 2025	unknown	Equifax Root CA
065c48a022926419df289003f69bd5ea	DigiNotar Public CA 2025	unknown	Equifax Root CA
729c841c5f39853b5a5166fcf0b679fd	DigiNotar Public CA 2025	unknown	Equifax Root CA
4a2242a78d5f52a864b4fdd8468ec2da	DigiNotar Public CA 2025	unknown	Equifax Root CA
b0ac4187e6c896a686b17082ecab4539	DigiNotar Public CA 2025	unknown	Equifax Root CA
c23cd54afd259fb7419c33f2f4d718e5	DigiNotar Public CA 2025	unknown	Equifax Root CA
408a3940773c44518e9429119f447066	DigiNotar Public CA 2025	unknown	Equifax Root CA
99b03a965285e290d42c54e5e47df153	DigiNotar Public CA 2025	unknown	www.Equifax.com



Appendix F
DigiNotar / Comodo

cert md5	ca	revoked	cn
fd2e074189200dc3331da2c6d88d16d2	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:21:11.000	*.*.com
c9606aa0c22b4d697d65e930407f8ab1	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:21:30.000	*.*.org
2dcba4384cabee90362da2a6ba69b843	DigiNotar Public CA 2025	unknown	*.comodo.com
1e451d680c17fadc3248d7e562e31da5	DigiNotar Public CA 2025	unknown	*.comodo.com
1c25fa64a0138514d444f65d4474abc3	DigiNotar Public CA 2025	unknown	*.comodo.com
e35c9abdd90517e6d3bf69ba14b0b8e1	DigiNotar Public CA 2025	unknown	Comodo Root CA
73e02d04264e0ed7329db7f520f5745f	DigiNotar Public CA 2025	unknown	Comodo Root CA
60162618e44882bbf075c095f7f43bb8	DigiNotar Public CA 2025	unknown	Comodo Root CA
ea7e11ddce415abf051d2ce1f33b16ea	DigiNotar Public CA 2025	unknown	Comodo Root CA
773c14c3c908c5daf6cb849547d2db26	DigiNotar Public CA 2025	unknown	Comodo Root CA
77c964debeaabd78636a129c637ce22b	DigiNotar Public CA 2025	unknown	Comodo Root CA
f48df880f9aa51da349cf1545860939d	DigiNotar Public CA 2025	unknown	Comodo Root CA
f4f86e5a661878ba6411fed7a14216ce	DigiNotar Public CA 2025	unknown	Comodo Root CA
61b5463724877ebb4825665f2ba9d8a7	DigiNotar Public CA 2025	unknown	Comodo Root CA
d61e9680f7ffe697a76e0e813cb3e3fd	DigiNotar Public CA 2025	unknown	Comodo Root CA
73de4f4c0397ad7aed05c9e28e87b16f	DigiNotar Public CA 2025	unknown	Comodo Root CA
904545d378575f226ae1622ca3429a5b	DigiNotar Public CA 2025	unknown	Comodo Root CA
2e4cb05503b040588ecaa99d35f9389b	DigiNotar Public CA 2025	unknown	Comodo Root CA
b1a7b0ee2d33310cfa7065cef60be8d1	DigiNotar Public CA 2025	unknown	Comodo Root CA
e91bb1e96bb870243d0720ce636748d3	DigiNotar Public CA 2025	unknown	Comodo Root CA
087c9f74c77e350edefab8b64d94bf47	DigiNotar Public CA 2025	unknown	Comodo Root CA
89cc580516c9671e3eb3703027643ffa	DigiNotar Public CA 2025	unknown	Comodo Root CA
5ea983ac95356b652b8237e91e7f4428	DigiNotar Public CA 2025	unknown	Comodo Root CA
f45aefcf9bedb1baff3c4faa06334699	DigiNotar Public CA 2025	unknown	Comodo Root CA
cf4ff9f230a982a67e2b9a2ace093a89	DigiNotar Public CA 2025	unknown	Comodo Root CA

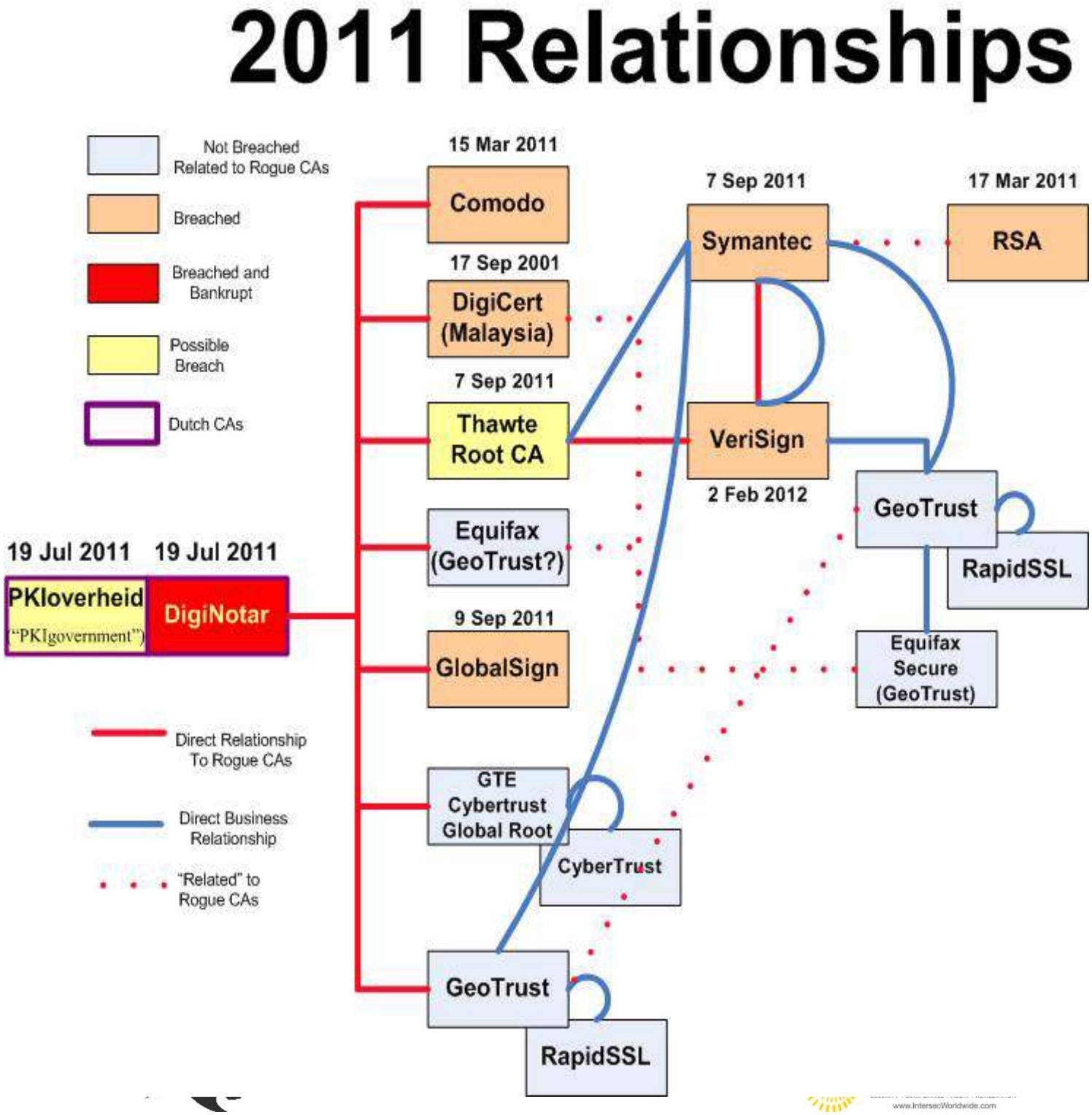
Appendix G
DigiNotar / DigiCert

cert md5	ca	revoked	cn
f4614f062b3162ba86364a9e993ba9f7	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:19:59.000	DigiCert Root CA
fd2e074189200dc3331da2c6d88d16d2	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:21:11.000	*.*.com
c9606aa0c22b4d697d65e930407f8ab1	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:21:30.000	*.*.org
3ca1132b6503c1091f94df951c43f72b	DigiNotar Public CA 2025	unknown	*.digicert.com
a10ad6f7aa35b2dd16594bcb7d9658e4	DigiNotar Public CA 2025	unknown	*.digicert.com
ff01dcd7df03712c5d8d1227a38a522c	DigiNotar Public CA 2025	unknown	DigiCert Root CA
e63a99035d0a8b9558a472aaf6be5e36	DigiNotar Public CA 2025	unknown	DigiCert Root CA
5f60791026749524O4bda6862ceea191	DigiNotar Public CA 2025	unknown	DigiCert Root CA
edab2d2c4c9140bce6cd07917bb756a0	DigiNotar Public CA 2025	unknown	DigiCert Root CA
eb00fbda220105e9bd43b91da50e4082	DigiNotar Public CA 2025	unknown	DigiCert Root CA
702dd25b9d7804b15442393b24a9c117	DigiNotar Public CA 2025	unknown	DigiCert Root CA
0fe1e4d76f13f6bbdb5ecb652b802533	DigiNotar Public CA 2025	unknown	DigiCert Root CA
eaad636a856230dc2dd7dc9a4a7f79ca	DigiNotar Public CA 2025	unknown	DigiCert Root CA
a44a0c5b116a484605ab0f66a04f440a	DigiNotar Public CA 2025	unknown	DigiCert Root CA
25ae58e8396ef0a5015ff08c91a32973	DigiNotar Public CA 2025	unknown	DigiCert Root CA
56b5733dc831f99b970789c834b91bd1	DigiNotar Public CA 2025	unknown	DigiCert Root CA
6cb43dc09b5e611193d388eb09eefc47	DigiNotar Public CA 2025	unknown	DigiCert Root CA
9fdd9a79524eead2f64b5705a3d831cf	DigiNotar Public CA 2025	unknown	DigiCert Root CA
a984383c14b5032af5a7318f5e968a62	DigiNotar Public CA 2025	unknown	DigiCert Root CA
0cf8bcf6af9d3d7b64e26ee389dc0122	DigiNotar Public CA 2025	unknown	DigiCert Root CA
f10a67884bf7e78ad08e9970dd7afc52	DigiNotar Public CA 2025	unknown	DigiCert Root CA
2c558ddf251d87587bac73a0bdcddf35	DigiNotar Public CA 2025	unknown	DigiCert Root CA
8e5a279a44c78011bcdde83cd329e974	DigiNotar Public CA 2025	unknown	DigiCert Root CA
8e31175ef671cdb80d42a13b5f212fd5	DigiNotar Public CA 2025	unknown	DigiCert Root CA
b78c9a3ec142f30961e8c081d653ec57	DigiNotar Public CA 2025	unknown	DigiCert Root CA

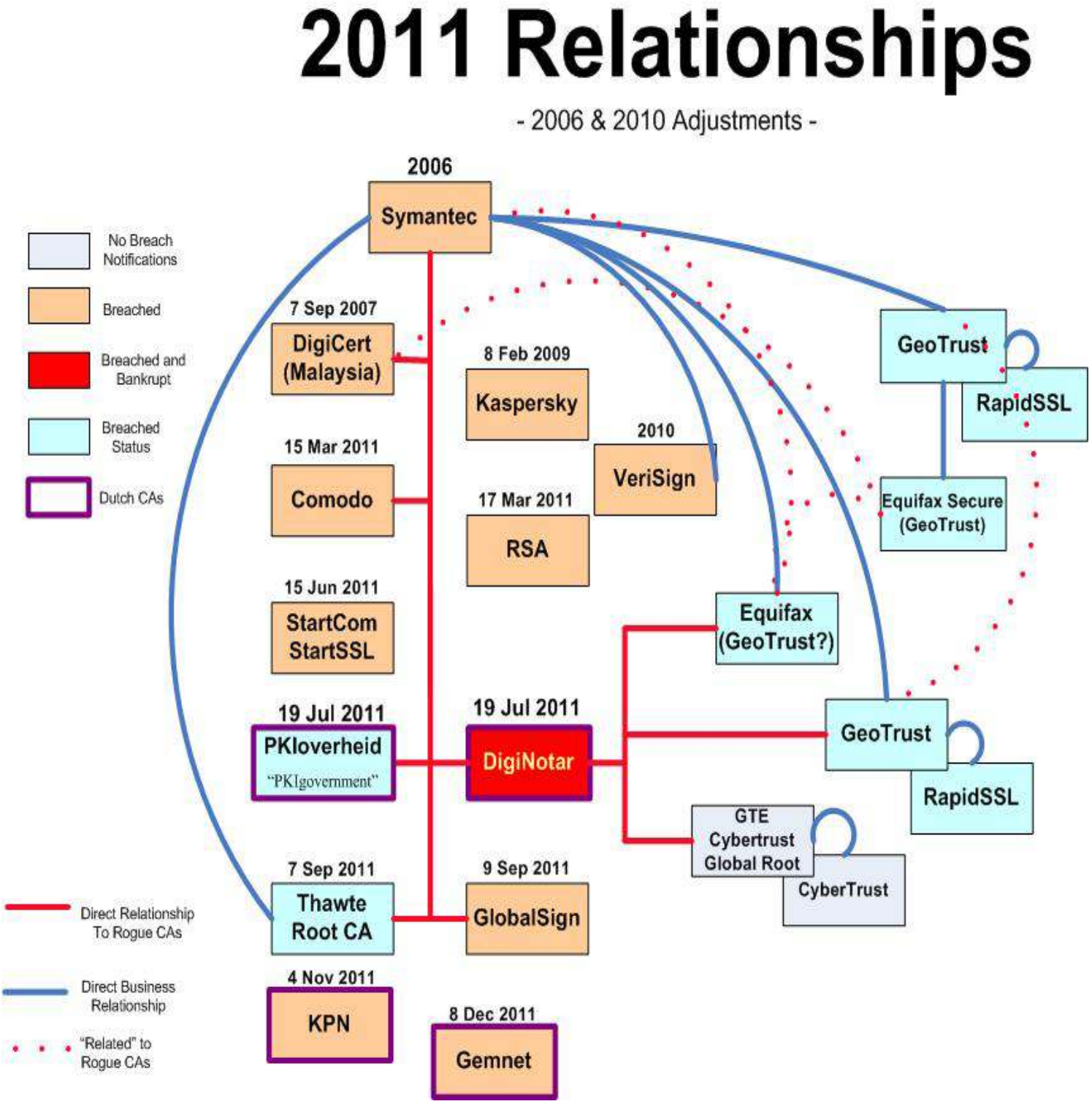
Appendix H
DigiNotar / GlobalSign

cert md5	ca	revoked	cn
fd2e074189200dc3331da2c6d88d16d2	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:21:11.000	*.*.com
c9606aa0c22b4d697d65e930407f8ab1	Koninklijke Notariele Beroepsorganisatie CA	2011-07-27 12:21:30.000	*.*.org
b7a884f4db1e8aa5d3c4a0db39e94a36	DigiNotar Public CA 2025	unknown	*.globalsign.com
11fcfad3bb3735cd42cb111e9ef45331	DigiNotar Public CA 2025	unknown	*.globalsign.com
13fdccb07123e7c4e672d155d192c611	DigiNotar Public CA 2025	unknown	*.globalsign.com
71998788b895e1e908c685919230c3f4	DigiNotar Public CA 2025	unknown	*.globalsign.com
c58e3bb670f789e7d3ce1b2520a506b6	DigiNotar Public CA 2025	unknown	*.globalsign.com
a71f3acaa083acfba1e5c1d4e08eeabe	DigiNotar Public CA 2025	unknown	*.globalsign.com
65e52a4d72bef020fb12c3b701655f1e	DigiNotar Public CA 2025	unknown	*.globalsign.com
1864d596116bc8010e18154edb2cfa90	DigiNotar Public CA 2025	unknown	GlobalSign Root CA
ea1fb28056344d41cc428628da037257	DigiNotar Public CA 2025	unknown	GlobalSign Root CA
ac23578a8dc1fbc8b5651dcd0edb3f1f	DigiNotar Public CA 2025	unknown	GlobalSign Root CA
796bb140de94d293afda1853b09c2971	DigiNotar Public CA 2025	unknown	GlobalSign Root CA
02d95a2be2b16de1a9cbca8f893596b8	DigiNotar Public CA 2025	unknown	GlobalSign Root CA
2f14b971f9b1c1ca1823de12e1c2ee3c	DigiNotar Public CA 2025	unknown	GlobalSign Root CA
9e7c0b0d1261141850db4418eabd6538	DigiNotar Public CA 2025	unknown	GlobalSign Root CA
5308506e64e39ad1446d11ec78937fd9	DigiNotar Public CA 2025	unknown	GlobalSign Root CA
a97ac35b345acc87e02827ee4de6defb	DigiNotar Public CA 2025	unknown	GlobalSign Root CA
85dcbe005fe39be338108f4890ce7b84	DigiNotar Public CA 2025	unknown	GlobalSign Root CA
cd59466215c1587285bb9366d77ec04c	DigiNotar Public CA 2025	unknown	GlobalSign Root CA
600eb5ab1f4baeec862c6b070221b5ef	DigiNotar Public CA 2025	unknown	GlobalSign Root CA
1e9652be292ae5138feca29860747ccb	DigiNotar Public CA 2025	unknown	GlobalSign Root CA
5aaf190de2b2e731537b41fb838a16cd	DigiNotar Public CA 2025	unknown	GlobalSign Root CA
39491e6b506726108e61d4cd0e88e865	DigiNotar Public CA 2025	unknown	GlobalSign Root CA
de5c8c956d149c61aa3772d805871266	DigiNotar Public CA 2025	unknown	GlobalSign Root CA
310b8d743a7a47338b0f2c47c891b06a	DigiNotar Public CA 2025	unknown	GlobalSign Root CA
dd7792271abc97cf3093e152e9aa76d5	DigiNotar Public CA 2025	unknown	GlobalSign Root CA
53c225c8a46c623730e50b36576629d3	DigiNotar Public CA 2025	unknown	GlobalSign Root CA
db5b64c4ea104258e36edff7eec45898	DigiNotar Public CA 2025	unknown	GlobalSign Root CA

Appendix I


2011 Relationships
Not Breached Related to Rogue CAs
Breached
Breached and Bankrupt
Possible Breach
Dutch CAs
15 Mar 2011
Comodo
17 Sep 2001
DigiCert (Malaysia)
7 Sep 2011
Thawte Root CA
Equifax (GeoTrust?)
9 Sep 2011
GlobalSign
19 Jul 2011
PKIoverheid ("PKIgovernment")
19 Jul 2011
DigiNotar
Direct Relationship To Rogue CAs
Direct Business Relationship
"Related" to Rogue CAs
GTE Cybertrust Global Root
CyberTrust
GeoTrust
RapidSSL
7 Sep 2011
Symantec
17 Mar 2011
RSA
VeriSign
2 Feb 2012
GeoTrust
RapidSSL
Equifax Secure (GeoTrust)

Appendix J



Appendix K
CA Breach Timelines