# Developing Shared Views for an Improved Public Key Infrastructure is Hard

Hannes Tschofenig*, Tobias Gondrom†
*Nokia Siemens Networks, Email: Hannes.Tschofenig@nsn.com
†Thames Stanley, Email: tobias.gondrom@gondrom.org

## I. Extended Abstract

High-profile data breaches and security incidents on the Web are gaining increasing attention from the public, the press, and governments. A few examples may illustrate the problems: DigiNotar, a Dutch certificate authority, had a security breach [1] and in the same year a Comodo affiliate was compromised [2]. Both cases lead to fraudulent issue of certificates and questions about the current strength of the security of the PKI architecture widely used in our web applications today. Also in 2011 LulzSec, a hacker group, claimed responsibility for several attacks, including the compromise of user accounts from Sony. Notifications about millions of stolen user accounts became common these days.

These developments have led to a number of activities to improve the security of the Web platform since the Web is in the front-line of these attacks. The IETF had started various standardization activities in response to these developments[1] We will mention a few of those and ask ourselves the question whether further work is needed.

The Web platform uses Transport Layer Security (TLS [3]) and relies heavily on the PKI for it's security. Consequently, a lot of attention has been paid on improving the cryptographic primitives and many valuable TLS extensions have been defined to improve security properties (e.g., cryptographic algorithm support, new credentials types). Unfortunately, the operational reality had not received the same attention. The public key infrastructure, as defined in RFC 5280 [4], assumed that certificate revocation lists (CRLs) or the Online Certificate Status Protocol (OCSP) [5] are used. Browser vendors do not seem to believe sufficiently in OCSP and CRLs or their constant and fully reliable availability and therefore they are not enabled per-default. The Certification Authority/Browser Forum [6], an organization of certification authorities and browser vendors, is largely responsible for today's operational practices of the Web PKI but acted prior to their organizational reform early 2012 operating behind closed doors. Many certificate signing practices (e.g., the existence of CAs with unqualified names, IP addresses and other artifacts) and the lack of accountability of CAs can be attributed to the policies in the CA/Browser Forum. The most important side-effect of the PKI model and the WebPKI, however, is the large number of trust anchors that can be found in today's browsers. While end users are at least theoretically in the position to modify the trust anchors, the lack of knowledge and the ability of browsers to delegate CA validation to external companies makes it almost impossible for end users to grasp the level of complexity and to judge who their browser trusts. The 2011 incidents have also shown that a single compromised CA can issue certificates for any Internet site since the name to key binding is not enforced in the PKI model. Some researchers and security experts call this a "design flaw", that any one weak entity in a very large number of hundreds of trusted CAs poses risks to the whole system and all users of the WebPKI. This situation also leads in game theoretic terms to disincentives for investments by each individual CA to improve their individual security posture. Although the IETF had even standardized a protocol for dynamically updating trust anchors (see TAMP [7]) it has not been widely used. Deciding which CA to trust and how many is just difficult; different stakeholders (e.g., end users, Website providers, browser vendors, CAs) have very opposing views.

The IETF had approached the topic in three directions:

1) develop an alternative to the PKI model[2] in the form of DNS-Based Authentication of Named Entities (DANE) [9], which re-uses the DNS to create the name to key binding. It does, however, rely on DNSSEC for it's operation and will therefore be a mid-to-long-term solution.
2) standardize shorter-term solutions in the Web Security (WEBSEC) [10] working group, such as the Public Key Pinning Extension for HTTP [11], HTTP Strict Transport Layer Security (HSTS) [12], TLS Channel Bindings [13], and alike.
3) document how the WebPKI currently works. The working group formation of the working group is in progress

Position paper for the 'NIST Workshop on Improving Trust in the Online Marketplace' , April 10-11, Gaithersburg, US. This paper represents the views of the author and does not reflect the consensus of the Internet Engineering Task Force (IETF), of any IETF working group, or of the Internet Architecture Board (IAB). Referenced documents may, however, reflect IETF consensus.

[1]While the title of the workshop is very generic our description focuses on activities related to alternatives to and improvement for the Web-based Public Key Infrastructure. Note that Public Key Infrastructure is not only used for the Web even though the Web infrastructure is the most visible application platform today. Other public key infrastructures may operate differently and may suffer from fewer or at least different problems. There are also problems related to improving on-line trust, such as the user authentication infrastructure, that are worth paying attention to.

[2]Note that there are also entirely different approaches for distributed authentication. For example, the Application Bridging for Federated Access Beyond Web (ABFAB) working group [8] focuses on a model that is closer to the AAA architecture, which is widely used for network access authentication.

[14]. The EFF SSL Observatory [15] may provide valuable input for this analysis.

In addition, the Certificate Transparency proposal [16] has been submitted to the IETF for publication as an RFC. It will serve as an experiment. as the authors describe it. Similarly to EFF's Sovereign Keys [17] the existence of an append-only log with all CA-issued certificates is assumed.

While the standardization work is progressing at a satisfactory speed, challenges remain. There is no common agreement of the design constraints and the types of threats that are supposed to be mitigated. While the authors of individual approaches have a strong view of how the future CA system should look like, there are subtle but significant differences between the existing proposals. For example, EFF's Sovereign Keys and the Certificate Transparency solutions do not want to place the same level of trust on the DNS as DANE does since the top-level domain operator may be under control of the attacker. Providing security for certain scenarios is in practical terms also extremely hard. For example, the coffee shop Internet access, Internet access via captive portal, enterprise , etc. Although the Sovereign Keys and the Certificate Transparency proposals are seen as an experiment it is not clear what the success criteria will be. Experiments are important but need to be refined to the right secure architecture as building the existing Web security infrastructure on an experimental infrastructure that may increase systemic dependencies or may otherwise be fragile could pose risks as well.

The authors would like to see the formation of an IETF or an IRTF working group[3] to discuss the proposed experiments to reach a better understanding of the design constraints and goals that should be accomplished. We believe it is important to involve a broad range of stakeholders; it will be a prerequisite for the success.

## REFERENCES


[1] C. Arthur, "DigiNotar SSL certificate hack amounts to cyberwar, says expert," Sep. 2011, guardian, URL: http://www.guardian.co.uk/technology/2011/sep/05/diginotar-certificate-hack-cyberwar.

[2] P. Hallam-Baker, "The Recent RA Compromise," Mar. 2011, comodo Group, URL: http://blogs.comodo.com/it-security/data-security/the-recent-ra-compromise/.

[3] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol - Version 1.2," Aug. 2008, Internet Engineering Task Force, RFC 5246, Request For Comments.

[4] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and T. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," May 2008, Internet Engineering Task Force, RFC 5280, Request For Comments.

[5] M. Myers, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP," Jun. 1999, Internet Engineering Task Force, RFC 2560, Request For Comments.

[6] P. Hallam-Baker, "The Certification Authority/Browser Forum," Mar. 2011, comodo Group, URL: https://www.cabforum.org/.

[7] R. Housley, S. Ashmore, and C. Wallace, "Trust Anchor Management Protocol (TAMP)," Aug. 2010, Internet Engineering Task Force, RFC 5934, Request For Comments.

[8] J. Howlett, S. Hartman, H. Tschofenig, E. Lear, and J. Schaad, "Application Bridging for Federated Access Beyond Web (ABFAB) Architecture," Oct. 2012, IETF draft (work in progress), draft-ietf-abfab-arch-04.txt.


[3]A few years ago the 'Public Key Next-Generation Research Group (PKNG)' [18] was created to discuss alternative PKI models but it had to be closed due to lack of interest.


[9] P. Hoffman and J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA," Aug. 2012, Internet Engineering Task Force, RFC 6698, Request For Comments.

[10] IETF, "Web Security (websec) Working Group Charter," Feb. 2012, URL: http://datatracker.ietf.org/wg/websec/charter/.

[11] C. Evans, C. Palmer, and R. Sleevi, "Public Key Pinning Extension for HTTP," Dec. 2012, IETF draft (work in progress), draft-ietf-websec-key-pinning-04.txt.

[12] J. Hodges, C. Jackson, and A. Barth, "HTTP Strict Transport Security (HSTS)," Nov. 2012, Internet Engineering Task Force, RFC 6797, Request For Comments.

[13] J. Altman, N. Williams, and L. Zhu, "Channel Bindings for TLS," Jul. 2010, Internet Engineering Task Force, RFC 5929, Request For Comments.

[14] "WebPKI Operations - Mailing List," 2012, Internet Engineering Task Force, URL: https://www.ietf.org/mailman/listinfo/wpkops.

[15] EFF, "The EFF SSL Observatory," Feb. 2013, URL: https://www.eff.org/observatory.

[16] B. Laurie, A. Langley, and E. Kasper, "Certificate Transparency," Oct. 2012, IETF draft (work in progress), draft-laurie-pki-sunlight-02.txt.

[17] EFF, "The Sovereign Keys Project," Feb. 2013, URL: https://www.eff.org/sovereign-keys.

[18] "Public Key Next-Generation Research Group (PKNG)," 2012, Internet Research Task Force, URL: http://irtf.org/concluded/pkng.