**WTPF-IEG/3/34**

OPINION X

Trust Frameworks and X.509 Certificates

The World Telecommunication Policy Forum (Geneva 2013),

*noting*

1. that through investment, development, and service delivery, the private sector plays an important role in the continued availability of Internet services;
2. that many of these services do not require and are provided with minimal regard to security;
3. that other services require trust frameworks and security mechanisms not present in the basic Internet Protocols,

*considering*

1. that X.509 certificates are an integral part of trust frameworks built on top of the basic Internet Protocols;
2. that a broad class of applications and services employ these frameworks and their trusted certificates to establish identities when communicating over secure channels such as Secure Sockets Layer (SSL)[[1]](#footnote-1) and Transport Layer Security (TLS)[[2]](#footnote-2);
3. that trusted certificates are issued by Certificate Authorities to entities wishing to establish trust and secure their communications;
4. that trust in the certificate ecosystem requires trust in all parts of that system;
5. that the strength of that trust is limited to the weakest link in the chain.

*further considering*

1. that trust stores are maintained on networked connected devices, e.g. end user machines, and are used to verify (trust) connections;
2. that end users rarely interact directly with certificates, trust stores, or certificate authorities;
3. that Certificate Authorities and trust store providers enjoy controlling positions in the certificate ecosystem;
4. that there is no effective mechanism for those that rely on trusted certificates and the trust frameworks they enable to ensure that those trust frameworks meet their needs.

*recognizing*

1. that there have been cases, where Certificate Authorities have themselves become untrustworthy;
2. that in at least one case[[3]](#footnote-3), this resulted in the release of fraudulent certificates into the ecosystem requiring trust store providers to reject certificates from that Authority with the subsequent failure of that Authority;
3. that the action of revoking trust in an Authority can have severe negative consequences on the legitimate users of that authority, resulting in either a “too big to fail” circumstance or severe negative externalities to customers and the international public at large.

*is of the view*

1. that better standards, best practices, and operating procedures could have prevented some “incidents”;
2. that without improvement and reform, catastrophic failure is no longer simply a theoretical possibility;
3. that given their central position in the security structure of the Internet, certificates, and in particular their issuance, require international collaboration and cooperation to ensure that those issuing them adhere to the highest standards and operate according to agreed principles and norms;
4. that international multistakeholder collaboration and cooperation is essential in advancing secure systems designed for the best interests of end-users.
5. that without such collaboration and cooperation, investment and development of security sensitive services may diminish.

*encourages and invites Members*

1. to consider constructive actions that would improve the X.509 certificate ecosystem;
2. to insist on a fully multistakeholder process for the development of standards, best practices, and norms;
3. to participate in such multistakeholder processes so as to ensure trust frameworks meet the needs of service providers and end users.
1. RFC 6101 [↑](#footnote-ref-1)
2. RFC 6176 [↑](#footnote-ref-2)
3. DigiNotar (http://en.wikipedia.org/wiki/DigiNotar) [↑](#footnote-ref-3)