03 December 2015

Subject: SAC075: SSAC Comments to ITU-D on Establishing New Certification Authorities

The Internet Corporation for Assigned Names and Numbers (ICANN) Security and Stability Advisory Committee (SSAC) has worked with various Transport Layer Security (TLS) certificate-related issues over the years. These include issues related to the use of public suffix lists for accepting wildcard certificates,[1] namespace collision issues with Internal Server Name Certificates and man in the middle (MitM) attacks,[2] and credential management.[3]

Today we have a web Public Key Infrastructure (PKI) system where any Certification Authority (CA) can, intentionally or unintentionally (e.g., as a result of a security breach), issue a fraudulent certificate for any domain name.[4] Adding additional root CAs measurably expands the attack surface of the system. The system is only as secure as the least secure or trustworthy CA in the entire set, any CA with a root certificate embedded in the relying party software represents a potential problem. As a result, the compromise or misbehavior of any one CA undermines the security and trust of the entire system. Furthermore, multiple root CAs in a PKI tethered to global name (i.e., Domain Name System (DNS) with DNS Security Extensions (DNSSEC)) or number space (i.e., Internet Protocol (IP) addresses and autonomous system numbers as with Resource PKI (RPKI)) puts the onus on a relying party to resolve conflicts or collisions that may occur, when the relying party may not possess information that would allow them to resolve such conflicts, particularly in times of instability.

As it relates to webPKI, the SSAC has been following and encouraging the evolution and deployment of the DNS, DNSSEC, and DNS-based Authentication of Named Entities

[1] See SAC057, SSAC Advisory on the Use of Static TLD / Suffix Lists, 15 March 2013 at: https://www.icann.org/en/groups/ssac/documents/sac-057-en.pdf.
[2] See SAC062, SSAC Advisory Concerning the Mitigation of Name Collision Risk, 7 November 2013 at: https://www.icann.org/en/groups/ssac/documents/sac-062-en.pdf.
[3] See SAC074, SSAC Advisory on Registrant Protection: Best Practices for Preserving Security and Stability in the Credential Management Lifecycle, 3 November 2015 at: https://www.icann.org/en/system/files/files/sac-074-en.pdf.
[4] See SAC057, SSAC Advisory on Internal Name Certificates, 15 March 2013 at: https://www.icann.org/en/groups/ssac/documents/sac-057-en.pdf.

(DANE). [5] We see a future in global trust tethered to the global name space and secured with DNSSEC as a better approach than solely secured with the multitude of root CAs that exist today. Thus, the SSAC believes standards based on DANE, possibly in combination with independent industry-developed solutions such as Certificate Transparency, are the future.

As such, we encourage interested parties to cooperate closely with the CA/Browser (CAB) Forum[6] and Internet Engineering Task Force (IETF).

Patrik Fältström
Chair, ICANN Security and Stability Advisory Committee (SSAC)

Attachment

[5] See RFC 6698, RFC 7218, and RFC 7671 at https://tools.ietf.org/html/rfc6698, https://tools.ietf.org/html/rfc7218, and https://tools.ietf.org/html/rfc7671.
[6] See https://cabforum.org/.

Telecommunication Development Sector
Study Groups

INTERNATIONAL TELECOMMUNICATION UNION
Second Meeting of ITU-D Study Group 2
Geneva, 7 – 11 September 2015

Document 2/252-E
11 September 2015
English only

Question 3/2:	**Securing information and communication networks: Best practices for developing a culture of cybersecurity**
SOURCE:	Rapporteurs for Question 3/2
TITLE:	Liaison Statement from ITU-D Study Group 2 Question 3/2 to ITU-T SG17 Q10/17, ICANN SSAC, AFRINIC, LACNIC, RIPE, ARIN, ISOC on PKIs and RPKIs for developing countries

Keywords: *cybersecurity, PKI, RPKI*

LIAISON STATEMENT FROM ITU-D STUDY GROUP 2 QUESTION 3/2 TO ITU-T SG17 Q10/17, ICANN SSAC, AFRINIC, LACNIC, RIPE, ARIN, ISOC ON PKIS AND RPKIS FOR DEVELOPING COUNTRIES

ITU-D Study Group 2 Question 3/2:
Securing information and communication networks: Best practices for developing a culture of cybersecurity

11 September 2015

To:	ITU-T Study Group 17 (Security) (Q10/17), ICANN SSAC, AFRINIC, LACNIC, RIPE, ARIN, ISOC
From:	ITU-D Study Group 2 (SG2), Question 3/2
For:	Action
Approval:	Agreed at the ITU-D SG2 meeting (Geneva, 11 September 2015)
Contact:	Ms Rozalin B.F. Al-Balushi, Oman Rapporteur for Question 3/2 Tel.: +968 9947 7755 E-mail: rozalin@tra.gov.om Mr Eliot Lear, United States of America Rapporteur for Question 3/2 Tel.: +41 44 8787525 E-mail: lear@cisco.com
BDT Focal Point:	Mr Marco Obiso BDT Focal Point for Question 3/2 Tel.: +41 22 730 6760 E-mail: marco.obiso@itu.int

ITU-D Study Group 2 Question 3/2 (Securing information and communication networks: Best practices for developing a culture of cybersecurity) received a contribution for consideration during its September 2015 meeting from the Republic of Togo (document 2/153), requesting that the impact and potential benefits of establishing root certification authorities in developing countries in order to elaborate a programme to implement such root certification authorities, if appropriate, be studied. As can be seen from the contribution, both Public Key Infrastructure (PKI) and Resources Public Key Infrastructure (RPKI) are mentioned.

ITU-D SG2 Q3/2 are contacting you because we understand that you may have already developed expert advice regarding the deployment of one or the other form of PKI. ITU-D SG2 Question 3/2 would be grateful for any information you have available on this topic.

Attachment:

Contribution 2/153 (Republic of Togo): Security of electronic transactions

Telecommunication Development Sector Study Groups
INTERNATIONAL TELECOMMUNICATION UNION
Second Meeting of ITU-D Study Group 2
Geneva, 7 – 11 September 2015
Document 2/153-E, 8 July 2015
Original: French/English
Question 3/2: Securing information and communication networks: Best practices for developing a culture of cybersecurity
SOURCE: Togo (Republic of)
TITLE: Security of electronic transactions
Action required: Document to consider in the final report
Keywords: Cybersecurity, electronic transaction, root certification authority

Abstract:

The Public Key Infrastructures commonly used to secure electronic communication services contribute to establishing confidence in the use of ICTs. Economic models stemming from their value chain can bring growth in the digital economy of the States that implement them. The ever-increasing development of electronic commerce and transactions, the progressive and large-scale deployment of new protocols and network services based on Public Key Infrastructures, and the security of the Internet of Things are, *inter alia*, reasons that should encourage the creation of root certification authorities in developing countries on the one hand, and the rethinking of a model of organization for the trust chain of the national-level root certification authority in a global way, on the other hand.

The objective of this contribution is to invite ITU-D Study Group 2 and ITU-T Study Group 17 to study the impact and potential benefits of establishing root certification authorities in developing countries in order to elaborate a programme to implement such root certification authorities, if appropriate. This study should enable estimation of developing countries' preparation for having a national root certification authority, and allow streamlining of the assistance that BDT is already providing, for instance on CIRT implementation.

Introduction

The development of electronic commerce and transactions, including online purchases and payments, execution of stock market orders, online administrative tax filing (VAT, income tax, electronic medical care sheet), exchanges of e-mails and electronic documents; the implementation of new network security protocols based on public key infrastructures and their progressive large-scale deployment, in

particular, DNSSEC, RPKI (Resources Public Key Infrastructure); and the security of the Internet of Things are crucial elements which should incite developing countries to work towards the establishment of institutions at national or regional level in charge of the management of their public key infrastructures. The creation of these institutions, if properly supervised, can contribute to strengthening the security of electronic communications in general, and that of electronic transactions in particular. They can also allow the emergence and development of digital economies in developing countries.

1. Statements

Electronic commerce and transactions are developing rapidly in developing countries. These transactions typically use insecure channels. However, when they are secured, they are based on self-signed certificates or on certificates purchased using certification authorities generally based in developed countries. In some cases, however, these certificates are not necessarily in accordance with the legislation of developing countries.

The lack of enthusiasm and the delays noted in the deployment of secure protocols, such as DNSSEC and RPKI, in developing countries are due to misunderstanding either of these protocols or the standards that allow their implementation, or to the insufficiently trained human resources involved in their deployment, or to a non-mastered grasp related to chains value.

All these inadequacies can be improved with the implementation of a root certification authority in each country. Indeed, the authorities, besides their traditional roles, will also be tasked with the broadcast, validation, and revocation of certificates to promote a culture of secure electronic transactions, as well as the organization of trust chains to national and international levels.

To assure this situation, some developing countries have set up root certification authorities. However, the functioning of these certification authorities does not necessarily reflect the state of the art in the field. It is advisable to improve the functioning of certification authorities, in particular, by implementing clear procedures based on best practices as well as accepted standards on the subject. This will have the advantage of ensuring the security of transactions and consumers in those developing countries that have already set up their certification authority on the one hand, and on the other hand, will promote the implementation of these certification authorities in those countries that do not have such capability.

Thus, in the context of the emergence of new digital economies in developing countries, the establishment of root certification authorities can be an important link and a social and economic development lever.

2. Proposal

This contribution aims at asking Q3/2 to undertake a study on the impact of the implementation of root certification authorities in developing countries.

The study should possibly lead to a proposal for the establishment of such root certification authorities in Member States, along the lines of what is currently being done with the setting up of CIRTs.

The objectives of the study include:

- assessing the readiness of developing countries for setting up root certification authorities at a national level;
- identifying requirements in terms of the skillset necessary to set up and run certification authorities at a national level;
- performing a gap analysis on the current national legal frameworks to better identify the actions required to improve national legislations on cryptography, digital certification and digital signature;
- reflecting on business models and operational plans to support the viability of the activities of the national root certification authority while taking into account regional specificities;
- assessing the possible evolution of national root certification authorities toward a chain of trust between them.

Furthermore it is requested that Q3/2 coordinate with ITU-T Study Group 17 to investigate the opportunity to:

- set up a human capacity-building programme for developing countries based on standards and the implementation of standards related to electronic certification, in particular the X.500 series standards;
- develop kits of best practices on the implementation and use of standards related to electronic certification.

3. Conclusion

The security of electronic transactions is fundamental in building confidence in the use of ICTs. The establishment of institutions whose operation should achieve this goal is essential for developing countries. However, it should be referenced by politically, technically and organizationally based frameworks that enable the creation and smooth organization of these institutions.