



ISOC-PKI Working Group White Paper Identification of ISOC members: PKI requirements

Status: FINAL

Feb. 26, 2003

Authors

Chiari, M.; Elamin, Y.; Gennai, F.; Hill, T.; Jarava, J.; Karttaavi, T. (ed.); Koltsoff, A.; Kummer, Z.; de Larrinaga, C.; Martin, P.; Nikander, P.; Orlando, F.; Rajan, S. V. (ed.); Tabanelli, R.; Soni, H.

Abstract

This paper is a discussion of the required elements for the identification of ISOC members specifically and limited to using PKI in such identification.

On-line version:

<http://www.isoc.fi/isoc-pki/whitepaper.html>

Table of Contents

1. Introduction.....	3
2. What is ISOC?.....	3
2.1 Organization.....	3
2.2 Chapters.....	3
2.3 Members.....	3
2.4 Elections and voting process.....	3
3. What is PKI?.....	4
3.1 Public Key Cryptography.....	4
3.1.1. Using Public Keys as Digital Proxies for People.....	4
3.2 Digital Signatures.....	4
3.3 Identity Certificates.....	4
3.4 Certificate Authorities.....	5
3.5 Identity PKI as an Infrastructure.....	5
3.6. Other types of PKIs.....	5
3.6.1. PGP Web of Trust.....	5
4. Need of PKI in ISOC.....	5
5. Organization of PKI in ISOC.....	6
5.1 Registration Office accreditation and audits.....	6
5.2 Directory Services.....	6
5.3 Certificate Revocation.....	6
6. Identification and verification process.....	7
7. References.....	7

1. Introduction

This paper is a product of the ISOC-PKI Working Group (<http://www.isoc.fi/isoc-pki/>). It discusses the use of Public Key Infrastructure to identify Internet Society (ISOC) members to ISOC, ISOC Chapters or other bodies relating to ISOC, when using electronic services. The paper also makes recommendations on the organization needed for the effective implementation of a PKI for ISOC.

This paper represents the consensus view of the members of the Working Group. It is to be read as a recommendation and does not necessarily reflect any views or policies ISOC might have on the issues discussed in it.

2. What is ISOC?

The Internet Society (ISOC) is a professional membership society with more than 150 organization and 11,000 individual members in over 182 countries. It provides leadership in addressing issues that confront the future of the Internet, and is the organization home for the groups responsible for Internet infrastructure standards, including the Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB).

2.1 Organization

The Society is governed by its Board of Trustees, which is elected by various constituencies. The executive function of the organization currently consists of officers (The ISOC Chairman, the President/CEO, Secretary, Treasurer and appointed Vice Presidents) supported by an administrative staff divided between Reston in Virginia and Geneva, Switzerland. The numbers in the staff are growing in line with the expansion in the activities of the Society and in the rapid growth in members. The interface to the Board of Trustees is managed through the Executive Committee.

2.2 Chapters

ISOC has a network of Chapters around the world. Chapters are financially self-supporting and have their own membership of individual members who are also by default members of ISOC.

2.3 Members

Any individual may join the Internet Society as a Global Member. This is a free membership available to anybody from the ISOC web site. Global Members may join one or more Chapters according to their own interests and Chapter rules. Chapters may have categories of memberships and may charge a membership fee.

2.4 Elections and voting process

ISOC By-Laws and Policies call for the Trustees to be elected or selected by various constituencies, namely Organizational Members, Chapters, and the IETF. Voting by Individual Members has been suspended since December 2001 when paid individual membership was superseded by a free Global

membership. A number of proposals are being considered for the re-establishment of a voting Individual membership constituency. The Board of Trustees itself is empowered to appoint a limited number of Trustees over and above the constituency-based Trustees.

3. What is PKI?

PKI, (Public Key Infrastructure), is a system that facilitates the distribution of public keys for Public Key Cryptography. It is an infrastructure to provide a secured environment to transfer data from one point to another, with allowed and verifiable identity. As there are many security infrastructures available, PKI provides us with a cohesive set of procedures and services to conduct a secured transaction. The PKI provides a complete life cycle management system in handling keys and certificates.

3.1 Public Key Cryptography

Public Key Cryptography or asymmetric cryptography, involves encrypting data using one key and decrypting the encrypted data using another key. Typically, people encrypt data using the recipient's public key, which only the recipient can decrypt as the owner of the corresponding private key.

All transactions should be signed. By so doing PKI gives the utmost confidence that a transaction is coming from a known party. To sign a transaction one needs a key. The key can be either a secret key or a public key. Secret key cryptography happens if both the parties have the same secret to use to encrypt and decrypt the information.

In public key cryptography the private key is a secret of the party who makes the request. So that other parties can send the information in a secured way, the requestor provides another key to everybody called the public key to encrypt the information. Once the requested information has been encrypted, only the private key can be used to decrypt it and reveal the clear text.

3.1.1. Using Public Keys as Digital Proxies for People

The public key will be generated for any entity based on the information provided to Certificate Authorities [3.4] after verifying the information. Hence, the public key can act as a digital proxy for that person. It is kind of identification card being presented without being there personally.

3.2 Digital Signatures

If it is to be trusted a public key needs to be signed by a trusted authority. Otherwise, one person can fake being another person. Whenever someone wants to make sure that the public key received is valid, he can interface with the issuing Certificate Authority to verify whether they issued the key, to whom it was issued, how long it is valid etc.

3.3 Identity Certificates

In Public Key Cryptography, digital certificates can be used to secure communication between two parties by encrypting/signing the data and/or by encrypting the communication channel. Identity

Certificates are used to facilitate the latter. They are used by entities to prove their identities to the recipients of the data that is using a secure communication channel (such as HTTP over SSL).

3.4 Certificate Authorities

Certificate Authorities are entities that certify owners of public keys. These entities issue digital certificates to requestors. Public key certificates are issued by the Certificate Authorities for a fee to the requestor after verification. The requestor can be a computer system or a person. The CA's are the foundation of PKI. They issue, maintain, verify, revoke certificates, and in some cases decrypt messages.

3.5 Identity PKI as an Infrastructure

The PKI as it is covered in 3.4, is a complete infrastructure itself. It helps to maintain the entire life cycle of the public key system. It is the basic source of trust for electronic transactions. For this to work firstly, people have to trust the CA if they are to trust the party they deal with. Secondly, the CA should provide all the mechanisms involved in the PKI world to deal with public keys. A CA has to address a broad range of issues from issuance of certificates to their verification. Other issues include scalability, maintenance, support etc. The provision of these services is what defines PKI as an infrastructure.

3.6. Other types of PKIs

3.6.1. PGP Web of Trust

PGP (Pretty Good Privacy), is an encryption system that allows people to communicate with each other securely. The PGP Web of trust is a model that certifies encryption keys by confirming people's identities through introduction by already verified members of the Web of trust.

4. Need of PKI in ISOC

Public Key Infrastructure has the potential to be useful to ISOC in helping to validate the identity of its members. The key applications where PKI might be useful are voting and access to private areas of ISOC web sites. The most notable election in ISOC is the election of Trustees to the ISOC governing body, the Board of Trustees. Chapters also follow similar procedures.

ISOC is a mixed membership organization with individual, chapter and organizational members. As mentioned above a fee paying individual membership ceased for the beginning of 2002 and has since been a free membership known as Global Membership.

Prior to this free individual membership, individual members only, elected the Trustees but they no longer can vote because the mechanism for verification (invoicing) of a Global member doesn't exist. The Trustees are now elected using a constituency model with each constituency assigned a number of board seats. The organizational members 6 Trustees, standards bodies IAB/IETF 3 Trustees, and Chapters 3 Trustees, with Chapter Presidents voting on behalf of their chapter.

Global members can be further subdivided into those who belong to a local chapter and those who do not. We can also take an alternate approach to having two kinds of members: people who are interested and people who are involved.

Those who are interested members regard ISOC as an information channel among others. They want to receive information, but do not participate actively. People who are involved typically belong to a Chapter (but not necessarily) and often serve as Chapter Officials. They participate in discussions, make initiatives and participate in working groups and committees locally and globally. In order to give those people more influence it is important to know who they are. In order to give people for example the right to vote, there has to be reasonable certainty that they do not vote with multiple identities. At the same time, those who are merely interested can carry on being on the mailing lists without having to go through any identification verification processes.

5. Organization of PKI in ISOC

The infrastructure includes the players, as described in chapter 3, and the processes by which they interact with each other. ISOC certificates are for internal use only, so the infrastructure is built on the existing organization. So for example, Users in this case are individual members, ISOC secretariat is the Certification Authority, Chapters are Registration Offices and Chapter's delegated persons are Registration Authorities. Every Chapter would initially have one Registration Authority, a person who is known to the ISOC central organization, or who can adequately verify her/his identity. This person, who in most cases is likely to be the Chapter President, can delegate the authority to another member or committee of the Chapter.

ISOC secretariat can also delegate the role of Registration Authority to trusted members of the Internet Society who are not members of any Chapter.

5.1 Registration Office accreditation and audits

Accreditation criteria for a Registration Office will have to be added to the criteria for forming a Chapter. ISOC will also publish operating guidelines for the Registration Offices. The operating guidelines will include accreditation criteria for Registration Authorities, which includes minimum requirements for identity verification. The Chapters are required to maintain a list of people who are accredited as Registration Authorities. The list includes names, ISOC ID numbers, contact information and a description of how their identities have been verified. Registration Offices are subject to audits by ISOC at all times.

5.2 Directory Services

Directory services can be managed by ISOC or outsourced.

5.3 Certificate Revocation

Certificates are revoked when the email address they are tied to expires or the certificate holder's membership is terminated. Any abusive or criminal use of the certificate constitutes grounds for

immediate revocation. Certificates can also be revoked and new ones issued if the integrity of the certificate is deemed compromised.

6. Identification and verification process

As the sign-up process needs to be as uncomplicated and straightforward as possible, the verification of identities should happen after one has become a member and only if one wants to enjoy privileges that apply to verified members only.

When a member wants her/his identity to be verified he/she requests a certificate from a local Registration Office (an ISOC Chapter). If this person is a paying member of that Chapter, no further identity verification is needed. If he /she is a Global Member without Chapter affiliation, or the Chapter in question does not charge membership fees, the applicant will need to verify her/his identity to the Registration Authority before a certificate will be issued. This requires a physical meeting with the Registration Authority (a Chapter's delegated person), presenting at least one form of legal photo identity documentation (e.g. passport, driver's license, national ID).

If a member requesting a certificate lives in an area where there are no Registration Authorities in the vicinity, s/he can verify her/his identity to ISOC by paying a verification fee.

The information bound to the certificate is:

- name
- email address
- ISOC ID

If a member changes the email address s/he uses within ISOC, then s/he will have to notify the CA of the change with an email message signed with the ISOC certificate. After verifying that the new email address is a valid one, a new certificate will be sent to the member.

7. References

Internet Society (2001). *Procedures for selecting Trustees*. [Online] Available HTTP: <http://www.isoc.org/isoc/general/trustees/select.shtml> [2001].