Contribution ID: **36** Type: **Oral Presentation**

A Study of Certification Authority Integration Model in a PKI Trust Federation on Distributed Infrastructures for Academic Research

Tuesday, 15 March 2016 14:20 (20 minutes)

Among certification authorities (CAs) in an academic PKI trust federation such as IGTF (Interoperable Global Trust Federation), most of academic organizations that operate CA install by themselves the CA equipment in their building. To keep CA trustworthy, it is necessary to maintain such CA equipment and to obtain the special operators. Consequently, the high cost of CA operation weighs heavily on the CA organization. For research institutes whose essential duties are not the CA operation, the burden on the high cost of CA operation is an earnest problem, and cost reduction with increasing the efficiency of the operation is an important issue.

In this paper, we discuss not further operational optimization of a single CA itself but cost reductions with an integration of more than one CA in a PKI federation. However, it is not easy to straightforwardly integrate CAs as follows: current CAs are turned into intermediate CAs, and a new root CA is built. This integration model would remain CA operation duties such as issuing, revoking, and identity vetting. Also, building the new root CA that covers different academic research communities would raise the total costs of CA operations. From the point of view of feasibility, the issues of CA integration are provided. As a solution to the issues, this paper takes notice of issuing and registration authorities constituting CA, and proposes the following integration model: it integrates the issuing duties, and each organization carries out the registration duties as before. In the proposed model, integrating the issuing duties means that one issuing authority (IA) takes over the duty of the other IA. Since each registration authority (RA) performs the registration duty as usual, most of procedures such as for application for certificate usage remain unchanged, so that it does not confuse the users.

Based on the idea of the proposed model, we discuss how to connect between the taken-over IA and the RA2 operated by the organization that closes its IA. Among possible connections, we examine not only direct connection between the taken-over IA and the RA2 but also connection putting the RA1 operated so far by the organization that operates the IA between them. Furthermore, we improve the certificate policy of the taken-over IA so that it is compatible with the policy of the RA2. We also discuss an applicability of existing CA profiles such as MICS (Member Integrated Credential Service) profile and its extension.

Primary author: Dr SAKANE, Eisaku (National Institute of Informatics)

Co-authors: Prof. AIDA, Kento (National Institute of Informatics); Mr NISHIMURA, Takeshi (National Institute of Informatics)

Presenter: Dr SAKANE, Eisaku (National Institute of Informatics)

Session Classification: Networking, Security, Infrastructure & Operations I

Track Classification: Networking, Security, Infrastructure & Operations