

# A Method for Remote Initial Vetting of Identity with PKI Credential

*Thursday, 9 March 2017 17:00 (20 minutes)*

With the growth of large-scale distributed computing infrastructures, a system that enables researchers – not only international collaborative research projects but also small research groups – to use high performance computing resources in such infrastructures is established. For the computing resource use system which invites researchers in the world to submit the research proposal, it is tough to carry out initial vetting of identity based on a face-to-face meeting at a window for the system if the researcher whose proposal is accepted lives in a foreign country.

The purpose of this paper is to propose a method to solve the difficulty of initial vetting of identity for a remote user.

An identity management (IdM) system vets the identity and reality of a user by checking the beforehand registered personal information against the identity documents. After the identity vetting, the user can obtain a credential used in the infrastructure. Suppose that the IdM system(A) needs to initially vet the identity of a user and that the user already possesses a credential issued by the other IdM system(B). The basic idea of this paper is that the IdM system(A) uses the credential issued by the IdM system(B) for the initial identity vetting if the level of assurance of the IdM system(B) is the same as or higher than the IdM system(A). However, the IdM system(A) cannot always check the identity against the attribute information provided by the credential. In a trust federation, the IdM system will be able to finish vetting the identity by making reference to the other IdM system that issued the credential for the necessary and sufficient identity data.

As the credential handled in this paper, we focus on Public Key Infrastructure (PKI) credentials that often used in large-scale high performance computing environments. We discuss necessary condition and procedure for ensuring that the remote initial vetting of identity with a PKI credential is the same assurance as the one based on a face-to-face meeting. The proposed method can be introduced to an existing PKI without large changes. The basic idea of the proposed method can be also applied to an infrastructure based on another authentication technology. The applicability of the basic idea is also considered.

**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:** Network, Security, Infrastructure & Operations IV

**Track Classification:** Networking, Security, Infrastructure & Operations