Universidad
Carlos III de Madrid

OO/UC3M/23 - AUTHENTICATION SYSTEM BASED ON ID-NETWORK SMART CARDS (ID-NSCARDS) FOR CRITICAL ENVIRONMENTS

Researchers in the Information Security area in the Carlos III University of Madrid (Spain) are interested to exploit the potential of an emerging technology: network smart cards. These new devices have a number of additional advantages for communications security in networked systems, comparing with the traditional smart cards. These interesting features could be applied to individual identification procedures in environments where critical tasks or operations take place. The required collaboration would be focused in the development and implementation of an authentication system for critical environments based on this technology.

Description and special features

Recently, smart cards have aspired to be considered as a common host within the network: Network Smart Card. Thus it must incorporate a variety of network authentication mechanisms and protocols to participate transparently in a heterogeneous networking context. Nevertheless, the authentication protocol design for smart cards has traditionally been oriented to support the functionality of a hardware token, as opposed to a design oriented towards the perspective of a host with network connectivity. Moreover, the smart card is overly dependant on the Terminal and this dependency is particularly undesirable when dealing with an unknown Terminal of questionable trust. Our work is focused on obtaining a high level of network integration and interoperability for the network smart cards, with the goal to develop robust systems for the identification and authentication of individual holding network id-cards. This approach is specially interesting when a critical scenario is considered. An efficient and effective authentication architecture based on id-cards is required in environments with critical operation or installations: hospital, nuclear, air-traffic or railway control or whatever low fault tolerant system.

As technological base, our research propose a remote authentication protocol architecture with the following characteristics:

- Stand-alone supplicant: We propose a new smart card remote authentication

model. The smart card adopts the functionality of stand-alone supplicant vs.
traditional split supplicant. This functionality is highly required in identification and authentication scenarios. In critical environments, the access Terminal should be considered untrustworthy and therefore additional security countermeasures are defined in our work.

- Atomic smart card authentication protocol design: the authentication protocol should be designed as an integral part of the smart card. We propose a specific protocol stack for a network id-card.

- End-to-end mutual authentication schema: the network id-card participates as a communication endpoint. On the opposite end, a centralized service controls the physical or logic access to the critical system. This authentication tunnel avoids attacks that are carried out by a manipulated access Terminal.

- Layer 2 authentication: our research aims to exploit the advantages for network smart card integration based on a layer 2 authentication scheme. We might implement lightweight communication protocol stack for these constraint devices, without lost of authentication robustness.

This project aims to specify and to develop an authentication system based on network smart cards with the previous features. This system will be specified for the robust identification of citizens or employees in critical environments.

Innovative aspects

Network Smart Cards is an emerging technology in study/prototype phase. There are few, although very interesting, works on this matter. Different strategies and approaches could be considered depending on the required final services. Our work is oriented to the exploitation of the layer 2 capabilities of the network smart card, with identification and authentication purposes. This fact favours backward compatibility with legacy smart cards, as well as, easy integration with a heterogeneous access network system (wired or wireless) and it provides communication interoperability with standardized networking protocols. This is a quite novel approach comparing with traditional smart cards or another techniques, which are based on a complete network protocol stack implemented in the smart card, with the goal to support common security protocols (SSL, IPsec, etc.). With our work, we aims to develop an specific system for identification based on these new ID-Network Smart Cards (ID-NSCards).

Competitive advantages

The deployment of this technology in a company or institution could have important competitive advantages related to the security of the system, and furthermore, to the reduction of time and costs in the maintenance and update of the involved security software and identity credentials. With the use of this technology, the identification and authentication of individuals or employees will be improved by means of a secure centralized service. An authentication system based on network id-cards allow us to provide robust mutual on-line identification and authentication procedures, as well as, the inter-working tasks (maintenance and software update, security policies, authorization attributes, etc.) between the network smart card and the remote authentication server. This end-to-end relationship implies that the Terminal/Host software is not modified and it favours the time and cost reduction. Furthermore, this fact allows us a dynamic, effective and very secure deployment, that is very required in these critical environments.

Current state of intellectual property: ☒ Patent applied

Technology Keywords

network smart card; ID-cards; ID-NSCards; Identification systems; ID&A; Authentication schemes; Communications security

Persona de contacto: María Dolores García-Plaza
Teléfono: + 34 916249016
E-mail: comercializacion@pcf.uc3m.es