Joseph Antonius Doekbrijder

Digitally signed by Joseph Antonius Doekbrijder
DN: CN = Joseph Antonius Doekbrijder, C = CH, O = SwissSign
Reason: I attest to the accuracy and integrity of this document
Location: Zürich
Date: 2004.07.06 14:57:04 +02'00'

Certificate Content

S W I S S S I G N D O C U M E N T

C O N F I D E N T I A L

Author: Joseph A. Doekbrijder, SwissSign AG

Introduction

The content of a certificate is public and should be able to identify a person “on-the-other-side” of a network as person allowed to access a service.

For this to work, every organization, (technically: server or service) that wants to use digital identities for authentication, needs to bind its information to the certificate: e.g. insurance policy, health information, (bank)account information, access rights or even social information like birthplace, residence, marital status, etc... All this information cannot be integrated in the certificate, since this information is not static and most of it is private!

The binding of a certificate to data is not part of PKI. With a PKI the organization does no longer have to manage the users passwords and can allow one certificate (=one user or “subscriber” in PKI terminology) to be bound to many different services. If a user is to be removed from accessing all these services it is only necessary to remove the link to the organizational data or to have the certificate revoked.

1 Privacy

In general should a certificate contain as little information as necessary. A certificate should not contain serial numbers or personal identifiers. It should also not contain “hidden” information (like year of birth) because with todays computer technology it will not be long before this hidden information is cracked and made public.

Still, it is necessary to have information in a certificate which makes the certificate unique. In order to prevent a human being from becoming a number it is necessary that a certificate contains variables that can be changed if the subscriber wants to.

Privacy needs to be upheld by the registration authority (RA) which has information about the subscriber that goes far beyond what is being published in a certificate.

2 Certificate content

The subject of a certificate is in PKI terminology referred to as distinguished name (DN). The DN usually contains information that allows for the identification of a person or service. The most used person identifying variable is called the common or canonical name (CN). A "common name" is a word or a phrase, without imposed syntactic structure, that may be associated with a resource. These common names are expected to be used primarily by humans (as opposed to machine agents)[1] which are often referred to as “canonical name”. SwissSign refers to the DN as: “digital identity”.

The preferred way to handle this uniqueness issue, is to include the subscribers email address in the subject of a certificate. Email addresses, are globally unique and need to be in the certificate anyway if the certificate is to be used to digitally sign email messages (RFC2632: “Receiving agents MUST recognize email addresses in the Distinguished Name field...”).

In addition a CN which should contain the complete name of a person (first name, middle names and family name) or a pseudonym.

Any other information is not necessary in the certificate! The RA has additional information which can be presented to a court if necessary.

[1] From the IETF Common Name Resolution Protocol (cnrp) Last Modified: 2002-09-18. See http://www.ietf.org/html.charters/cnrp-charter.html

3 The mechanism

How does it work?

As mentioned before, every organization that wants to use digital identities for authentication, needs to bind its information to the certificate: e.g. insurance policy, health information, (bank) account information, access rights or even social information like birthplace, residence, marital status, etc... All this information cannot be integrated in the certificate, since this information is not static and most of it is private!

To protect the privacy of this additional data, it must be maintained decentralized in databases where the main lookup key (besides the ca) is the subject DN (never use the public key or the certificate number since it is likely to be changed whenever a smart-card or crypto token is lost or renewed).

This way the certificate (better= digital identity) is reduced to a unique name that helps looking up other data, but it does not reveal any private information. Further, the elements in the DN, email address together with a name (real or pseudo) are a globally unique pair than can be changed whenever the subscriber wants to prevent data mining.

4 Compatibility

As presented above, these certificates would be internationally compatible and as such work with all RFC conform applications.

5 Proposal

SwissSign proposes that Swiss qualified certificates (certificates build according to the stipulations of ZertES) contain in the subject an email address together with a name (real or pseudo). This makes these certificates unique and allows the certificate owner (subscriber) to get a new digital identity whenever he or she wants to.