DRAFT

A privacy friendly certificate for communities: The Community Certificate

Abstract

Keywords

Introduction

[motivation]
One of our friends told us that he was asked to prove his age before allowing him to access an adult only web site. This site demanded his credit card information for age verification. He posed a question to us. He asked why he should give that much information to prove his age and he also stated that a credit card is to buy goods services on credit, but not to prove one's age. This inspired us to think about a promising solution for both netizens and online shoppers. Since, providing the requested information poses at least two threats; the site may charge a fee, mishandles ones personal information. Is a credit card a proper mean of demonstrating one's age or any other attribute? What about others who do not have credit cards? Surveys show netizens are reluctant to reveal privacy sensitive information. Are not there promising means for demonstrating possessions of attributes on the internet? i.e. showing one or more attribute(s) without disclosing other attributes especially one's identity.

[previous approach]
The RFC 3281 has categorically listed two difficulties in incorporating other attributes (identity is one attribute) in a Public Key Certificate (PKC). But, this paper explores the possibility and benefits of having attributes in a public key certificate. This paper explains how insignificant the given two grounds are and how to overcome those limitation in a more efficient and attractive manner.

[approach]

This paper proposes a new kind of digital certificate which facilitates netixens to demonstrate their possession of attributes in a more privacy friendly manner. It proposes to extend the optional extension field defined in the third version of the PKC (RFC 2459). The other suggestion is to make two optional messages in RFC 2246 mandatory. In other words, making the client authentication phases compulsory. Apart from those two suggestions, the paper explores both technical infrastructure and operational procedures required for implementing a practical Certificate Authority (CA).

[overview]

First, it looks at the existing public key infrastructure and its limitation. Then, it goes on to a discussion on the desired features and practical issues of a privacy friendly digital certificate scheme. The next section explains the proposed solution which suggests various combinations, short term and long term implementations, and operational

procedures. The discussion section examines the advantages and the applications of the proposed solution. This paper concludes by suggesting some future research areas.

Related work

In the paper based world, a paper-based certificate is used to demonstrate the possession of certain attributes. For example, a birth certificate is used to show the date of birth. The corresponding mean in the digital world is a digital certificate. However, the PKC has very limited attributes, only identity attributes. The PKC is defined

which is linked to the corresponding identity certificate. The identity certificate is defined in http://www.itu.int/rec/T-REC-X.509-200508-I . which binds the holder's public key to one of his claimed identities. Every public key has a corresponding key called private key which is kept under the custody of the public key holder. The general assumption is that non one else can use it. The concept is quite similar to a hand signature or an official seal. The private key owner is responsible for the use of it. On the other hand, a public key is known to others. The process of binding a public key into an identity is the main task of a Certificate Authority (CA). It gets a hash value of the public key and other identity data and digitally signs the hashed value by its signature key. If one trusts the CA, he can get the public key and verify the CA's signature. After relying on the genuineness of the public key, the verifier sends a challenge and asks the certificate holder to sign the challenge using his private key. Once he gets the signed challenged, he can very the proof of possession of the private key, if the public key successfully decrypts the signed challenge. In some case, a CA handles only the issuing process and delegates the assurance process to another authority. It can be seen four classes of PKCs based on these attributes and the attribute verification process. For example, a Class 1 PKC demonstrates that the holder has access to the email account specified in the PKC. Class 2 shows the real identity (in this case the name of the holder) with a simple mean of verification process such as inspecting a fax photo id. The next level, which is Class 3 PKC has the same information but the verification process is more strict. Common verification processes are 1) getting an assurance certificate from person whose trustworthiness has already been well established, Web of Trust (WoT) 2) getting an assurance certificate from a trusted third party such as public notaries, lawyers, charted accountants etc.. The most advanced verification process, which requires checking military background or financial credibility, gives Class 4 PKCs. The attribute certificate is intended to define many attributes. One limitation of PKCs is limiting only to a name or an email address. It is required to demonstrate the possession of more attributes than just a name and an email address.

Attribute Certificates

The Attribute Certificate (AC), which has a similar structure as the PKC except for the absence of the public key, was introduced in the early 1990s to fill this gap . The AC has given three options to link to the PKC. The rationality was to that one has to prove the identity before granting him the rights to access the resources: First authentication then authorization. Even in the physical world, most of the time, it is required to prove the authenticity of the claimant before granting him the authority to access resources. The three given options are 1) baseCertificateID field is assigned the serial number of the holder's PKC 2) PKCs.entityName which links to a name or role of the holder 3) objectDigestInfo which links to a digest of the information of the holder. RFC 3281, which defines the specification of the AC, gives two reasons for having a separate specification for the AA and not putting it as an extension of the Public Key Certificate (PKC). One reason is that the lifetime of an attribute is not the same as lifetime or the identity. The second reason is that the authority or ability of the PKC verifiers to certify the possession of attributes. Our study and our experience at CAcert convinced us that these two problems can be solved by issuing the free certificates, and only charging for the identity and attribute verification. It has also shown that the cost of issuing short life time certificates is bearable. Other advantages of separating the AC from the PKC are that the AC can independently renewed and keep the length of the PKC short. However, Browsers, Webservers, CA Software and protocols (SSL/TLS) would have to be rewritten to put AC into practice.

Chaum's credentials

David Chaum also proposed a credential system without having a public key. In this system, one organization uses digital credentials which state that the holder has possessed the mentioned attributes. His proposal is based on his concept of blind signature. However, Brands has listed a number of problems associated with this concept in designing attribute certificates . Some of those criticisms are that *Chaum's credentials* do not support negotiation of privacy, impossibility of encoding expiry dates, relying on a central party, possibility of replaying messages etc..

Open Profiling Standard

This stands was to submit personal information (attributes) to web servers. A user maintains his personal profile in his local computer or a remote server, when web sites request personal information, the user decides which of the information that is stored in his profile should be sent to the server. This standard was subsumed by P3P in 1998. This concept is quite similar to Microsoft´s CardSpace (InfoCard) system.

Platform for Privacy Preference (P3P)

This facilitates a user to negotiate his privacy preferences with web servers. The standard supports to define machine readable privacy profile of users and privacy practices of web sites. This machine readability makes it possible to negotiate privacy preferences without human interaction.

PKCS 6
This standard supports to have additional attributes (compared to PKC). It also provides backward compatibility. However, the validity period is restricted to the life time of the shortest attribute.

Brand's work – He proposed a digital credential mechanism to have a privacy friendly attribute certificate. His proposal contains advanced mathematical techniques. One of the promising grounds in cryptography is the proper establishment of mathematical concepts (rewrite with references). This paper discusses a promising approach which is based on the existing Public Key Infrastructure (PKI). However, Browsers, Webservers, CA Software and protocols (SSL/TLS) would have to be rewritten to put Brands credentials into practice.

Dr. Stefan Brands has invented a new mechanism for certificates that can contain attributes, where each of the attributes is only presented on demand. Additionally, queries on attributes are possible, it´s possible to proof that the value of an attribute is in a certain range, without disclosing the value itself.
Pros:

- Solves the Privacy problems

Cons:

- Browsers, Webservers, CA Software and protocols (SSL/TLS) would have to be rewritten.

6th Option: OACerts

OACerts are an invention of Jiangtao Li and Ninghui Li, which uses a Bit-Commitment protocol to commit the attributes into the certificate, so that the user can choose for each attribute whether he wants to disclose the committed attribute or not.

[System Model]

The Problem

One of the significant features in digital documents is the capability of storing and processing of information in a few seconds for few cents. This creates serious privacy threats. For example, a custom officer looks at a passport and face of the holder to make sure authenticity of the holder and the holder was given permission to enter into the country. He compares the facial picture on the passport and true face of the holder to authenticate the holder. He then looks at the visa stamp/sticker to get to know the permission given him by a migration authority. But, he is not interested in the name field of the passport. Here we can see the perfect balance between security and privacy. However, if a digital medium is introduced instead of a security officer, it is possible to store movements of passengers. The stored data may be processed for various other purposes apart from preventing illegal immigrations. Here, people feel this excessive

security is a threat to their privacy. These are the instances where people show their reluctances to reveal their true identities due to potential privacy and security threats where they feel that the excessive security is a threat to their privacy. Once (Personal Information) is revealed, they do not have (or have a very limited) control over the collected data. The privacy notice does not guarantee proper handling of the collected information. There are many countries which are yet to enact data protection legislatures. This indicates the importance of an authorization scheme which does not require the identity of the holder in the digital world.

The PKC, which contains the identity of the holder, does not to solve the problem at all. According to Brands, digital identities are more invasive than paper based identity documents and more usage encourage identity theft.

There are many commercial and non commercial CAs. However, it is hard to find an Attribute Authority which certifies the possession of attributes. Some of the reasons may be the complexity of the structure of the AC and practical difficulties in assuring the possession of attributes.

Operational challenges

- For example, Brands suggests putting confidential attributes into the digital credential to prevent sharing the certificates. His solution is theoretically sound but the practicability is highly questionable.
- Another success factor is the cost of implementation and operational cost. A business cannot be initiated without having a fair ROI.
- It is not possible to operate an anonymous systems credential system without an anonymous payment system. Since the payment details can easily be traced and a link can be established.
- Other challenging issues are going beyond boarders of a country, building a trusted assurance network around the globe etc.?.

Requirements

The following are the requirements for potential solutions:

R1. Several Attributes can be shown by a user at the same time
R2. The user has the control over the presentation of the attributes to a relying party
  R2.1. The user can decide for each attribute to show or not to show it
  R2.2. The attributes are not sent in plaintext to the relying party
  R2.3. The relying party does not need any connection to the issuer
  R2.4. Several relying parties can´t easily combine their data about users
R3. An efficient revocation infrastructure is possible/available
  R3.1. The revocation infrastructure does not disclose any information to a third-party
R4. The system can be implemented reusing the currently available infrastructure of the Internet (Browsers, SSL/TLS, ...)

R5. The system is compatible with the existing services
R6. The attributes are digitally signed by a CA
R7. Usability

	R1	*R2.1*	*R2.2*	*R2.3*	*R2.4*	*R3*	*R3.1*	*R4*	*R5*	*R6*	*R7*
X.509								Yes	Yes		
X.509+Ext	Yes	No	No	Yes	No	Yes	~	Yes	Yes	Yes	
X509+AC	Yes	Yes	Yes	Yes	No	Yes	~	Yes	Yes	Yes	
OACerts	Yes	Yes	Yes	Yes	No	Yes	~	Partly	Yes	Yes	
U-Prove	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes	Bad
credlib	Yes	Yes	Yes	Yes				No	No	Yes	Bad
SAML				No							
CardSpace	Yes	No								Optio	

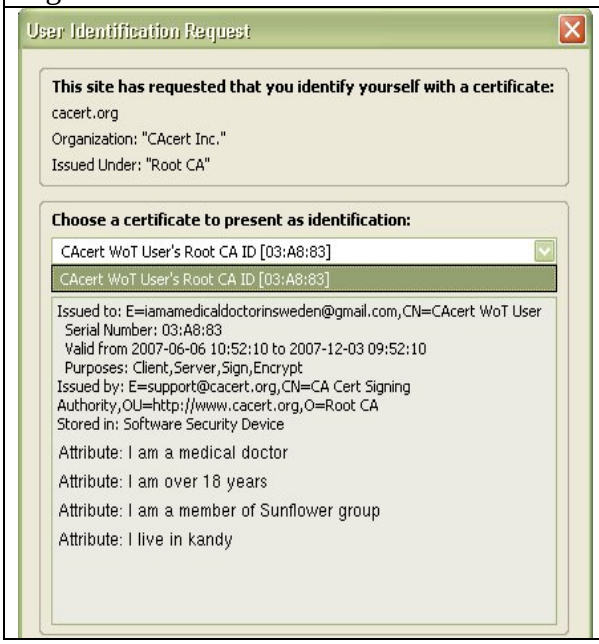
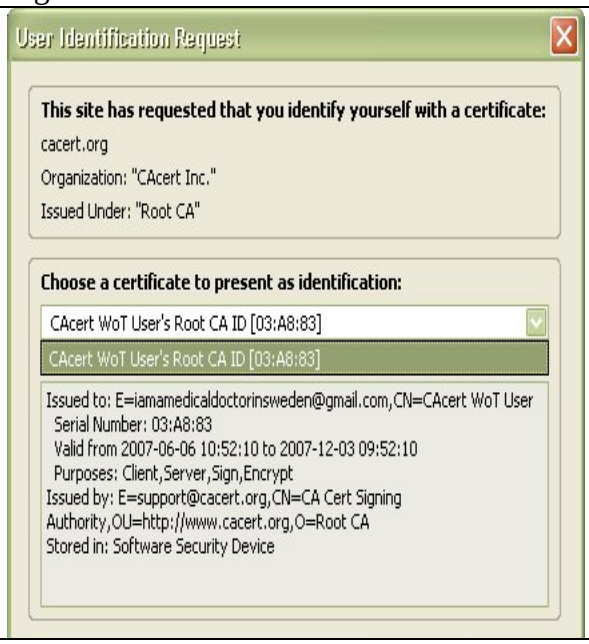
Solution

The solution to the problem is to extend the optional extension field defined in the third version of the PKC (RFC 2459) and making the two optional messages in RFC 2246 mandatory. The following options, which are arranged according to complexity, give the realizations approaches together with pros and cons. The proposed technical details are given under technical section while operational details are presented in operational procedure section.

Here, the identity attribute is filled with a common name such as 'WoT user' and the email address attribute can be kept blanked, filled with a bogus email address or have a common email address.

Option 1

The simplest and quick solution is to have a single CA and extended digital certificate (community certificate) with multiple attributes as shown in figure 1.

Figure 1	Figure 2
	

Pros:

- It works with the existing software and protocol infrastructure (Browsers, Webservers)
- It requires only a single, existing CA (compared to other solutions) and a number of extensions in the certificate.
- It does not require a completely new user-interface in the browsers, but slight improvements would be helpful.
- The certificate can be used as a normal identity certificate too
- A single communicate certificate may contain more than one value for a single attribute.

Cons:

- The user always presents all attributes when showing the certificate
  - For example, one wants to prove his locality but his authorization certificate also contains his professional attribute. Sending this certificate reveals unnecessary information. In this case, it is his professional status.
- SSL/TLS currently sends client certificates in plaintext over the wire, revealing the attributes to anyone listening in the traffic. So it is not recommended to do it this way because of this privacy issue.
- It is not compliant to the Attribute-Certificate RFCs
- Since a single CA with multiple attribute reveals the presence or absence of many attribute and their values to the receiving party.
- The attributes can only be issued by a single CA, so a user can´t use several attributes from different CA´s at the same time.
- It may require frequent updates since there are a lot of attributes in a single CC.

Option 2

A CA is set up with OU=Community.CAcert.org and O=CAcert Inc. The first part of the OU field (i.e. Community) is used to differentiate a community CA from an identity CA. The same applies for digital certificates. This CA generates different kind of certificates with the same DN (i.e. OU=Community.CAcert.org and O=CAcert Inc). For example, location community certificate, professional community certificates. Figure 1 gives a list of attributes and possible combinations of them.

Pros:

- This authority could issue different kind of CCs (Community Certificates)
- A single community certificate may contain more than one value for a single attribute. For example, in the case of a requestor plays multiple roles such as a medical doctor, a lawyer, an accountant etc., the same attribute field is multiplied with different values.
- It makes it difficult to link the transaction of the holder since attributes are scattered around multiple public keys.
- A CC can easily be renewed without verifying other attributes.

Cons:

- When a user gets a number of CCs, this approach becomes uneasy for the user. He has to go through all CCs to select the right one. The existing browsers help very little in identifying the right FC. Figure 1 and 2 shows how IE and Mozilla present their pop up boxes when a web server request a digital certificate. Mozilla is much better compared to IE since it gives a summary in the bottom panel. IE requires a user to open and read the content of a FC.

Figure1: Internet Explorer Popup

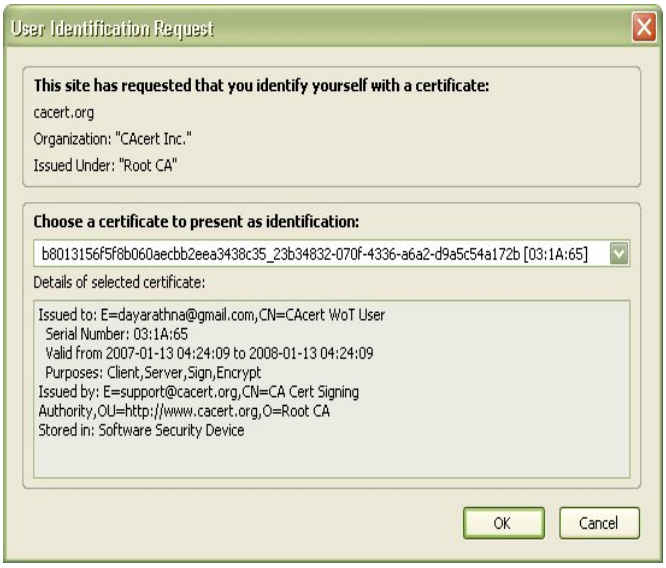


Figure2: Firefox Popup

Option 3

One solution to limit number of CCs to be chosen is having a chain of CAs with different Distinguished Names (DN) as shown in table 1. Since, a browser filters digital certificates based on acceptable CAs' list sent by a web server in the certificate request message in the TLS or SSL handshake. There is a trade off between resource allocation at the server site and user friendliness at the client side.

- Having a unique DN is very helpful for a user, since he gets a few ACs.

Cons:

- There is a scalability problem at a server site. Since, it is technically or organizationally not possible to handle a large number of CAs by a single organization. However, a few CAs are manageable.

OU field	Description
Location.CAcert.org	location (residential area, home town, working place) of the user
Profession.CAcert.org	profession of the user (e.g. medical doctor, engineer, clerk, accountant)
Age.CAcert.org	The truncated age of the user.
Professional.CAcert.org	**Whether a user belongs to a designated category of professionals.**
Membership.CAcerr.org	memberships the user has
LocationProfession.CAcert.org	defines both profession and location of the user

Table 1

Table 1 lists the defined OU names and description thereon. As shown in the table, it is possible to have combinations of attributes. For example, the attribute Location.Profession defines both profession and location of the user. The professional attribute has a Boolean value. i.e Yes/No.

Option 4- Improvements

The promising solution is option 2. However, the existing browsers make it uneasy for users in selecting the right community certificate among many. This is due to the fact that the existing browsers do not display attributes and their values in a user friendly manner. Therefore, a user has to open the certificate and read through the list of fields to identify the right one.

Today, a server can only signal which CA´s it demands, not which attributes. This can be improved in such a way that the server could use the TLS protocol to signal to the client which attributes it demands, so that the client can present only those certificates that contain the requested attributes. This improves user friendliness. One possible approach is encoding the required attribute(s) in the name list of the allowed CAs' in the certificate

request message in the TLS/SSL handshake phase. This encoding is done by specifying the required attribute in the OU field. For example, when a location certificate is required, the OU field is set to location.CAcert.org. The browser parses the OU filed and gets the type of attribute requested by the server. It then filters digital certificates based on acceptable CA list and the parsed attribute value.
However, the price for a user to get an attribute verified is so high that it´s unlikely that a user will get more than a few certificates with attributes, so we don´t need a further selection.

Pros:

- Easy

Cons:

- Bad usability for a larger amount of certificates

Improvement option 2:
Define a TLS extension for the signalling
...

Improvement option 3:
Abuse the OU fields in the DN of the CA list for signalling

Technical detail

- **The structure of the proposed authorization certificate**

The proposed structure for the authorization certificate is a slight extension made to the PKC v3 (RFC 2459) standard. The extension field is used for defining attributes. When issuing a CommunityCertificate, the newly defined extension field is filled with attributes value. The following figure shows the structure of a PKC. The highlighted extension field is used for defining attributes, their criticality, and values.

```
Certificate  ::=  SEQUENCE  {
     tbsCertificate       TBSCertificate,
     signatureAlgorithm   AlgorithmIdentifier,
     signatureValue       BIT STRING  }

TBSCertificate  ::=  SEQUENCE  {
     version         [0]  EXPLICIT Version DEFAULT v1,
     serialNumber         CertificateSerialNumber,
     signature            AlgorithmIdentifier,
     issuer               Name,
     validity             Validity,
     subject              Name,
     subjectPublicKeyInfo SubjectPublicKeyInfo,
```

```
        issuerUniqueID  [1]  IMPLICIT UniqueIdentifier OPTIONAL,
                             -- If present, version shall be v2 or v3
        subjectUniqueID [2]  IMPLICIT UniqueIdentifier OPTIONAL,
                             -- If present, version shall be v2 or v3
        extensions      [3]  EXPLICIT Extensions OPTIONAL
                             -- If present, version shall be v3
        }
   Extensions  ::=  SEQUENCE SIZE (1..MAX) OF Extension

   Extension  ::=  SEQUENCE  {
        extnID      OBJECT IDENTIFIER,
        critical    BOOLEAN DEFAULT FALSE,
        extnValue   OCTET STRING  }
```

Here the max value is set to one in the option 2 and 3 since there is only one extension present in a CommunityCertificate. The extnID represents the OID value of the attribute and the octet string extnValue is used to set the value of the attribute in the ASN.1 encoded structure.

OU field	OID	Example value
Location.CAcert.org	1.3.6.1.4.1.18506.6.1	Sweden
Profession.CAcert.org	1.3.6.1.4.1.18506.6.2	Doctor
Age.CAcert.org	1.3.6.1.4.1.18506.6.3	43
Nationality.CAcert.org	1.3.6.1.4.1.18506.6.4	SE
MemberOf.CAcert.org	1.3.6.1.4.1.18506.6.5	CAcert Inc.
SecurityClearance.CAcert.org	1.3.6.1.4.1.18506.6.6	ISA-TOP SECRET
KnowsAbout.CAcert.org	1.3.6.1.4.1.18506.6.7	Computer
CustomerOf.CAcert.org	1.3.6.1.4.1.18506.6.8	SnakeOil Ltd.
SupplierOf.CAcert.org	1.3.6.1.4.1.18506.6.9	Healthcare
Possesses.CAcert.org	1.3.6.1.4.1.18506.6.10	Car

Table 2

Table 2 lists the proposed OU fields and their corresponding OID values.

Another modification is done to the key usage field. The digitalSignature bit and non-repudiation (bit 1) are asserted since the subject public key is used for a digital signature mechanism and to provide a non- repudiation service. **?!?!?!?**

- **The structure of the proposed authorization protocol.**

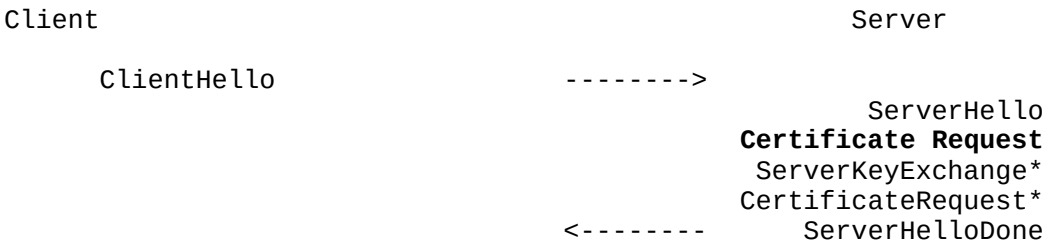


Fig. 1 - Message flow for a full handshake **(RFC 2246)**

*Indicates optional or situation-dependent messages that are not always sent in the TLS protocol.

Two optional certificate messages to and from the server in the TLS protocol have been made compulsory in the proposed handshake mechanism for the authorization certificate. The first message which comes from

?!?!?

Operational procedures

- Requesting an Authorisation Certificate(AC)

Once a user requests for an authorization certificate, the CA starts its verifying process to assure that the requester has the requested attribute. The verification and assuring process is explained under “assurance process”. If the assurance process is successful, then, the CA issues a AC which contains the requested attribute. The certificate can be password protected. The user can download the certificate and store it in his browser or hardware token. This process is exactly similar to the identity verification process carried out by CAs.

Kinds of ACs

A combination of different attributes and attribute verification process provides a basis for three different kinds of authorization certificates. The following section discusses three different combinations of attributes and various mechanisms of certifying the possession of requestors’ attribute.

Three versions of authorization certificates

- Authorization certificate with identification information
- Authorization certificate with pseudo identification information
- Authorization certificate without identification information

Authorization certificate with identification information

A user requests an AC from an Attribute Authority (AA). An email is sent to the requestor’s mail box to make sure that the requestor has access to the mail box. Then, the requestor has to convince the AA that he has possession of the requested attributes. There are two means of convincing. They are Trusted Third Party (TTP), and Web of Trust

(WoT) assurance processes. In the TTP mechanism, generally, lawyers, bank managers, notaries, charted accountants are considered as trusted third parties. In the TTP assuring process, the requestors has to meet at least two trusted third parties who are willing to certify the possession of attributes of the requestor. The particulars of the TTPs , their consent for assuring the requestor and obtaining their particulars from their professional bodies should be sent to the AA by the TTPs themselves. Their eligibility is verified by online directories and confirmations obtained by professional bodies. Then, application for attribute assurance forms are sent to them via a courier service. This application form consists of two parts; one is for the particulars of the requestor and the second part for the TTP. Once the TTPs assure the requestor, he is required to send the completed application form to the AA together with certified copies of the identity certificate and the certificate of attributes. For age verification, a copy of the birth certificate and identity certificate. Then, a link to download the attribute certificate is sent to the mailbox. Now, the requestor can download the certificate and store it in his certificate repository. The digital certificate contains both identity and attribute(s) information.

The other process is called “Web of Trust” (WoT) assurance process where the requestor meets at least three (depending on their trust level) assurance parties. An assurance party is a party whose trust level has already been certified and given authority to certify new requestors by the AA. They can follow the assurance process described below and inform the AA the eligibility of the requestor.

Attribute certificate with pseudo identification information

The process is similar: Under this scheme, TTPs or Wot assurance parties keep the copies of identity and attribute certificates. In case, the document in custody is revealed under strict conditions. This revealing process requires the consent of both the AA and the parties who have certified the requestor.

Attribute certificate without identification information

The process is the same except a few modifications. Here, the requestor can ask the AA for an attribute only attribute certificate. In this certificate, the name field is filled with a common name such that it is not possible to identify the holder. The email address is a bogus email address which is created only for the time taken to obtain an AC. The TTP or WoT assurance party informs the AA the eligibility of the requestor without any identification information. The requester should make sure not leave any document with the TTP. This is not called a perfectly anonymous AC since it is possible to trace the certificate holder. But, it is expected that the identification process may be costly.

The Assurance Process

Both TTP and Assurance party mechanisms must follow the instructions given by the AA. In verifying attributes, special attention should be paid to the life time of the attributes. The following table shows some attributes and their life time:

Attribute	Life time
Name	During the life time (except a name change)
Date of Birth	During the life time of the holder (no exceptions)
Profession	This depends on many factors. However, this is a life time attribute in many cases. One exception is disbarring someone by a professional body.
Studentship	Until one finishes his studies
Age	At most one year
Nationality	During the life time (except changing nationality)
Top title	At most until the end of job contract

- Presenting an Attribute Certificate

Once a user attempts to access an attribute protected web site, he is asked to present an authorization certificate having a particular attribute. The user can select an authorization certificate stored in his browser or any other hardware token. If the chosen authorization certificate is password protected, a pop up box appears and request the correct password to access the certificate. Once the correct password is provided, the certificate is transferred to the requested web server. Upon verification of the attribute, the site/server allows the user to access the resources. If a user wants to have anonymous communication, he must send the data and his certificate through an anonymized channel.

Discussion and Analysis

It was decided not to name this proposal as "Attribute certificate" since the RFC 3281 has already used that name. It has also mentioned that an AC is one means of authorization mechanism which convey privileges from a holding entity to another entity . This led us to use "features certificate". Cambridge Advanced Learners Dictionary defines it as an important part of something. Here, the important parts are attributes and something is the holder.

A comparison between a PKC and AC.

The AC can be used to digitally sign messages, encrypt messages, and authenticate clients and servers. A user can do all above operations without revealing his identity but only showing his attribute. Users do not need to understand the concepts, technology and mechanisms behind the new AC infrastructure nor need to have new software to manage the AC.**!?!?!** This process is quite similar to the existing PKI.

A relying party can link all the messages sent by a particular sender based on the unique serial number contained in the AC.

Unlike the attribute certificate, the proposed authorization certificate does not contain a link to an identification certificate. There are two plus points. If a user wants to reveal his identity, he can use a single certificate. If he does not want to reveal his identity, he can use a certificate without any identification information.

It is required to have a study on the applicability of the existing legal provisions relating to the PKI on the proposed authorization scheme. However, it the similarities of the two systems may make it possible to apply the same legal provisions with slight modifications.

A user can prove having more than one attribute by sending two attribute certificates. For example, Mr. A can send his residence attribute certificate and his professional attribute certificate. These certificates reveal where Mr A is from and what he is. For example, the former reveals his is a Swedish while the second one reveals that he is a doctor. The cumulative effort shows that Mr A is a medical doctor in Sweden.

This is a better solution for restricting children entering web sites. Some children tend to steal credit card information from their parents. They may use the credit card information not only to enter a porn site but also to get some services from online shoppers. The certificate can be password protected. This protection prevents children accessing the certificate. A credit card does not provide a similar protection. The card itself reveals all the information necessary to make a payment using the card.

This enables a particular group of people to communicate without revealing their identities but showing a common attribute. For example, medical doctors can have a discussion without revealing their identities but everyone knows that he is communicating with a medical doctor. This may enable them to share their experience, opinions, etc. in a more democratic manner.

Advantages

- Either the unique number or the public key in the certificate can be used for many purposes. One is grouping or arranging messages/transaction based on the unique number. This arrangement gives all dealing carried out by a user. This same number (let say the unique serial number) can be used to deny access to a web site or services. When a user becomes disgusting, his right to access the web server can be denied. If an anonymous user is denied, he can obtain a fresh certificate. If the certificate contains an identifier, the denying web server can ask the issuing CA not to issues any more certificate to that particular user.

- Users prefer customized web sites since it is more convenient to choose preferred options. Customization enables organizations to provide a better and more effective service. However, it needs a unique identifier to customize the site. On the other hand, organizations collect unnecessary personal information for their commercial gains. Surveys have shown that people are reluctant to provide their personal information. The usual practice is providing bogus information (i.e. pretending to be some one else) to web servers which is not a promising solution. For example, it is time consuming and difficult to remember previously used identities. Microsoft introduced InfoCard system which facilitates to demonstrate different identities. However, showing wrong identities is ethically highly

questionable. But, the feature certificate gives a promising solution. Have a feature certificate with loyalty attribute (i.e. amazon loyalty). This certificate facilitates organizations to customized web pages based on the unique identifier in the certificate and visitors can protect their personal information. A customer can negotiate with an organization what information the organization wants and benefits given to the visitor. This helps to improve the quality of data gathered by the organization.

- One of the techniques for limiting the sharing of certificates is restricting it to a given number of times or a usage duration. For example, it can be said that a certificate can be used only once per day. This is only applicable in some cases such subscription to online magazines etc.. For example setting the attribute to <TheSundayTimes_1> enables the holder to use the certificate only one per day. Instead of number of times, it can be set to number of hours or days. This is highly practical since the holder sends a digitally signed request. Therefore, he can't latter deny it.How does that work? Where did you read that?

Some possible applications

```
* Being a journalist
* Having security clearance Level x
* Being member of club x
* Having knowledge about topic x
* Being customer of x
* Being supplier of x
* Being inhabitant of x
* Possessing a x
* Has credit rating x
```

Future works and Conclusion

The proposed mechanism lacks certain desirable features. Those are

- An ideal system should not reveal information more than a user disclosed even in the case of colluding of certificate issuer, relying parties, verifiers with unlimited computer power .
- It is not possible to send more than one features certificate at a time. If one wants to demonstrate the possession of two attributes which are in two different FEATURES certificate. However, the alternative is obtaining a features certificate containing both attributes.

- One of the most critical issues is the possibility of sharing digital certificates. The solution proposed by Brands, which is encoding confidential information about the holder is not practical without a strong governmental enforcement. It is doubtful who is willing to have his confidential information in the proposed digital credential. Digital Rights Management (DRM) may give a good solution.

- One possible threat is unnecessary demanding a features certificate. If one does not provide his certificate or the provided certificate contains one or more attribute which the receiver does not like, the holder may be subject to discrimination. This is beyond our scope and it requires an involvement of legal privacy advocates.

- Another interesting point is looking at possibilities of embedding features certificates into a smartcard or similar hardware token.

- If ones identity is revealed, it is possible to trace all his past usage of the certificate.

(OID 1.3.6.1.4.1.18506.6)

Rasika Dayarathna and Philipp Gühring