Using Notary Based Public Key Infrastructure in Shibboleth Federation

Hendri Nogueira[1], **Ricardo Felipe Custódio**[1], **Cristian Thiago Moecke**[2], **Michelle S. Wangham**[3]

[1]Laboratório de Segurança em Computação (LabSEC)
Universidade Federal de Santa Catarina (UFSC)
Caixa Postal 476 – 88040-900 – Florianópolis – SC – Brasil

[2]SecUSo - IT Security, Usability and Society
Center for Advanced Security Research Darmstadt
TU Darmstadt
Mornewegstraße 32 – D - 64293 Darmstadt

[3]Grupo de Sistemas Embarcados e Distribuídos–GSED/CTTMAR
Universidade do Vale do Itajaí(UNIVALI)
São José, SC, Brasil

{jimi,custodio}@inf.ufsc.br, cristian.moecke@cased.de, wangham@univali.br

Abstract. *The X.509 Public Key Infrastructure contains many services such as Registration Authorities, Time Stamping Authorities and Certification Authorities, that increases its complexity, redundancy and difficulties of implementation for a digital certification. Notary Based Public Key Infrastructure (NBPKI) is a model that eliminates the redundant processes, complexity and brings many facilities for the authentication processes. This work describes the use of NBPKI model combined with a Credentials Translation Service to improve the Shibboleth Authentication Process.*

1. Introduction

Public Key Infrastructures (PKIs) provide the capability of establishing a trusted relationship between the entities involved in a digital transaction. PKI is used for digital signature, secure network communication, on-line transactions (E-commerce), authentication, digital identity, to protect data with encryption and others [Lancaster et al. 2003].

PKI is normally formed by entities that detain a pair of asymmetric cryptographic keys. The private key is securely maintained and controlled exclusively by its owner, and the public key is shared with the others. Some types of these models are PGP (Pretty Good Privacy), SPKI (Simple Public Key Infrastructure) and IBC (Identity Based Criptography). The most used model is X.509 [Cooper et al. 2008].

The increased use of X.509 PKI has led to a series of limitations and difficulties related to its implementation [Linn 2004]. In a typical X.509 PKI environment, the verifier of a digital signature needs to check: the time-stamp signature; the validity of the Time Stamping Authority certificate and its certificate chain, including the revocation information at that time; the signatory certificate validity and all certificates in its certificate chain, revocation information based on time-stamp date and the document signature.

These verifications need excessive human and computational resources to maintain and provide long-term trustworthy services. To deal with these and others limitations, Moecke et. all [Moecke 2011] proposed a new PKI model (NBPKI - Notary Based Public Key Infrastructure), that uses self-signed digital certificates and substitutes the Certificate Authority (CA) with Notarial Authorities (NA).

Differently from Moecke who focused his model in digital signature, this work focuses on another use of Notarial Authorities – Federate Authentication. This paper describes the use of self-signed certificates to improve the Shibboleth Authentication Infrastructure. The solution combines NBPKI - a model that eliminates the redundant processes, complexity and brings many facilities for the authentication processes - to an Identity Provider with additional functionalities in order to make possible to a user of federation, through desktop application or browser, authenticates using a self-signed certificate. The proposed model supports authentication credentials translation.

The remainder of this paper is structure as follows: section 2 reviews the typical authentication credentials for academic federations based on Shibboleth framework; section 3 explains some questions relating to NBPKI; section 4 presents some related works; section 5 describes the use of NBPKI in Shibboleth Federation; and section 6 concludes the paper and describes the future works.

2. Federated Authentication and Authorization Infrastructure

Academic Federations are collections of educational and research institutions and organizations that have agreed to inter-operate using a common set of rules, particularly in the areas of privacy and security. Federations make the use of standard methods for authentication and authorization and single sign-on technology [Internet2 2011b]. They define the trust relationship, the policies used for exchanging information, software to enable authentication and authorization, and distribute the metadata necessary for interoperability.

The federated identity technology allows organizations and institutions with an economically efficient and convenient way to manager and deliver identity services between different organizations, helping deal with user and data security on the same network [Don and Smith 2008].

A Federated Authentication and Authorization Infrastructure (AAI) includes Service Providers (SP) and Identity Providers (IdP). IdPs maintain identity databases and authenticate users. The SPs are responsible for authorize the accesses and do not need to maintain user databases.

There are many academic federations around the world, like FEIDE, InCommon, SURFnet, CAFe and many others. CAFe Federation is from Brazil and managed by RNP (Rede Nacional de Pesquisa) [RNP 2011]. Like others federations, CAFe uses the Shibboleth framework [Internet2 2011d] as authentication and authorization infrastructure.

Shibboleth is a project [Scavo and Cantor 2005] initiated from Internet2 [Internet2 2011c], an advanced networking consortium led by the U.S research and education community. The Shibboleth architecture defines a set of interactions between IdPs and SPs to facilitate the browsing of attributes' exchange and single sign-on authentication through web browsers [Cantor 2005]. Shibboleth is based on the SAML (Security Assertion Markup Language) standard [OASIS 2011].

The Shibboleth framework implements both sides of the federated communication (IdP and SP) and a central service responsible for obtaining the information about the IdPs registered in the federation and performing the redirect that is called WAYF (Where Are You From?) or DS (Discovery Service).

Figure 1 shows the typical communication flows in a Shibboleth Federation. The communication for a user that accesses a service for the first time, occurs with the following steps:

1. The user attempts to access a Shibboleth-protected resource on the SP site.
2. The service redirects the user's browser to the WAYF service.
3. The user selects his institution from the list presented by the WAYF. He is redirected to his IdP.
4. The user authenticates to the home IdP, using his *username* and password, for example.
5. The IdP generates a one-time handle (session identifier) and sends it to the user's browser, then redirects to the SP. Sometimes the SP needs to request others attributes information from the IdP to authorize his access. The IdP, on the basis of its Attribute Release Policy, allows or denies attribute information to be made available to this SP.
6. Based on the attribute information made available to it, the SP allows or refuses the user access to the resource.

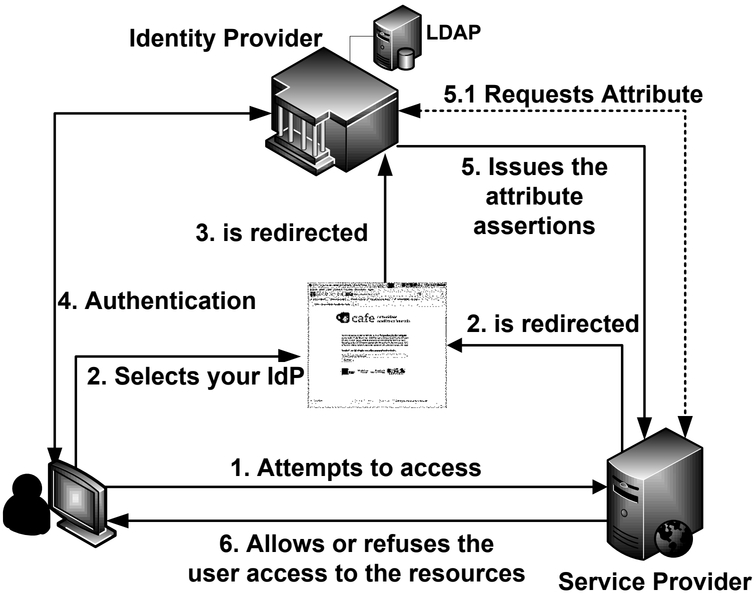


Figure 1. Communication flows in a Shibboleth Federation

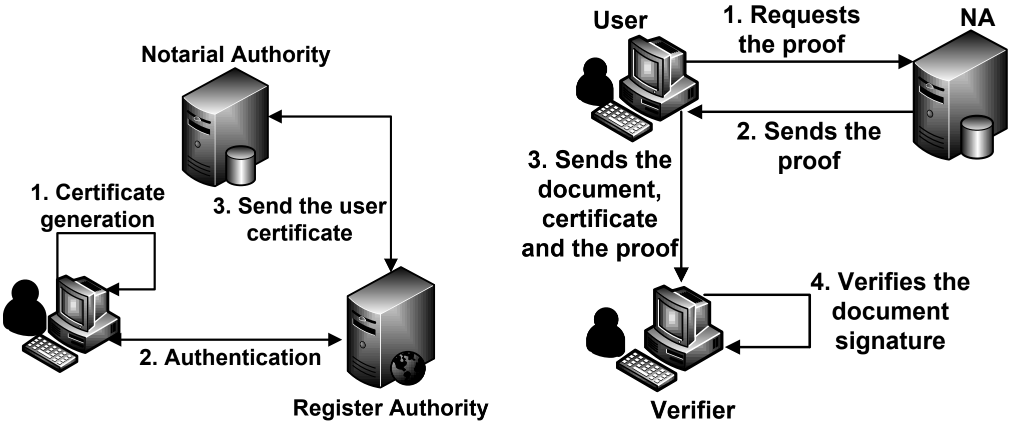
3. NBPKI

NBPKI (Notary Based Public Key Infrastructure) is a new approach of PKI, which through its simplicity, becomes adequate for signing electronic documents without losing the generality of a PKI [Moecke 2011]. It does not propose new cryptographic algorithms as IBC [Shamir 1984], CLC (Certificateless Cryptography) [Al-Riyami and Paterson 2003], CBC (Certificate Based Cryptography) [Gentry 2003], and does not propose any change in the X.509 standard. This model proposes a new structure and organization in X.509 PKI, based on the same cryptographic algorithms already widespread, tested and used in X.509 PKIs.

This model uses the approach of self-signed certificates [Moecke et al. 2010] and consequently does not have any certificate chain. The proof of the certificate's validity is only necessary on the date of verification.

This indicates that it is not necessary a Certificate Authority (CA) to issue the certificate. The proof should provide sufficient evidence to confirm the information in the certificate. The certificate format is similar to the X.509 model, so the X.509 standard can be used in this model.

In the NBPKI model, two authorities are proposed [Moecke 2011]: the Registration Authority (RA) and the Notarial Authority (NA). This model needs the existence of at least one entity responsible for the issue of the self-signed certificate proof – the NA in which the role is similar to a CA.


Notarial Authority
1. Certificate generation
3. Send the user certificate
2. Authentication
Register Authority
User
1. Requests the proof
NA
2. Sends the proof
3. Sends the document, certificate and the proof
4. Verifies the document signature
Verifier

(a) Self-signed certificate creation.

(b) Verification of a digital signature with the certificate proof

Figure 2. Self-signed certificate and the validation proof

The RA has a similar role to the RA in X.509 PKI. In this model, the user can generates his own self-signed certificate and makes the communication to the RA through a secure authentication to prove his identity and the possession of his private key. The RA verifies the information of the certificate and then sends it to the NA. The NA stores the certificate in the database and it is ready to issue the user certificate proof.

The Figure 2(a) shows the generation of the self-signed certificate. The user can also go to a RA entity, prove his information, and get his self-signed certificate and private key on a secure hardware.

After the NA receives the certificate from the RA, the NA needs only a simple and automatic process to register the certificate in its database. When requested, the NA is responsible for issue the proof at an exact instant in time. As there is not a certificate chain in this model, the user/system does not need to build and checks the certificate chain.

When the user needs to validate the integrity of a certificate, he needs to obtain one valid proof from the NA. The proof can be obtained by the user and dispatched to the verifier (user or service) or solicited by the system. The Figure 2(b) shows how the verification of a digital signature is in the NBPKI environment [Moecke 2011].

A NA verifies the certificate's status in the database and returns the proof, which is called a *token*. The *token* contains the revocation situation of the certificate, that is valid or invalid at that time. As the *token's* validity is short, this model can dismiss the use of a revocation mechanism to validate the *token*, proposed by Rivest and Elisson [Rivest 1998, Ellison et al. 1999].

The date is included in the *token* by the NA by a trusted clock, similar in what happens in Time Stamping Authorities. This makes the date safe as well as the Notarial Authority when issuing the proof. The use of self-signed certificates for the authentication brings less complexity of certificate verification and no necessity of certificate revocation list.

4. Credential Translation

The Shibboleth framework does not provide the integration of different types of authentication credentials, such as X.509 credentials used to grid applications. Besides that, in a federated environment, the Shibboleth [Cantor 2005] permits only that communications among the user, the IdP and SP occur only through the web, i.e, using web browsers and HTTP protocol. As a result, many services provided by other organizations can not be integrated in Shibboleth Federation.

Some works proposed alternatives to integrate services that supports different authentication methods, by SAML credentials translation into other types of credentials, like X.509 certificates. Mello [de Mello et al. 2009] proposed a model based on the Credential Translation Service that allows SSO authentication where even heterogeneous security technologies are considered. Mello's proposed model provides authentication credentials translation and attribute transposition, involving different kinds of credentials and permissions in the federation environment.

There are many projects that involve a new infrastructure that enables the integrations from different AAI technologies and bringing better the interaction and security for management and exchanges of the information, like Project Moonshot [Howlett 2011] and CILogon [Directorate 2011].

Wangham [Wangham et al. 2010] proposed an infrastructure that aims to offer new features to Shibboleth Federations. This work is being developed in the context of GT-STCFed project [Wangham et al. 2011], funded by RNP (NREN who manages the Brazilian federation - CAFe). The features provided by the infrastructure are the translation of authentication credentials and federated authentication to non-web applications. The infrastructure of the GT-STCFed pilot project is composed of two services: the STS (Security Token Service) and CTS (Credential Translation Service). The STS consists of a Web Service that has the function of issuing and validating security credentials, according to the WS-Trust, WS-Security and WS-Policy specifications.

The STS acts as a gateway between trusted identity providers in a Shibboleth Federation and non-Web applications. The CTS deals with aspects of translation of credentials between different security technologies and is always invoked by the STS when the application requires a security credential (eg. X.509 certificates) different from that used by the federation. STS and CTS are integrated into the IdP, composing an IdP with additional features (called IdP+). This IdP+ can be accessed by a web service client (desktop application), not only via a Web browser.

5. The use of NBPKI in Shibboleth Federation

In academic federations, IdPs acts like RAs, generating key pair and issuing the certificate for theirs users at the moment of the user's registration. In this paper, it is proposed a service (RA) that creates the private key and a self-signed certificate at the user station, based on the user information at the IdP database.

This model by using communication protocols of web browsers needs to communicate to an IdP that has the support of be linked to the RA service for mapping the certificates parameters through SAML assertion. This different IdP structure is called IdP+ and the RA is implemented at the same server as IdP+ because the flows are simplest.

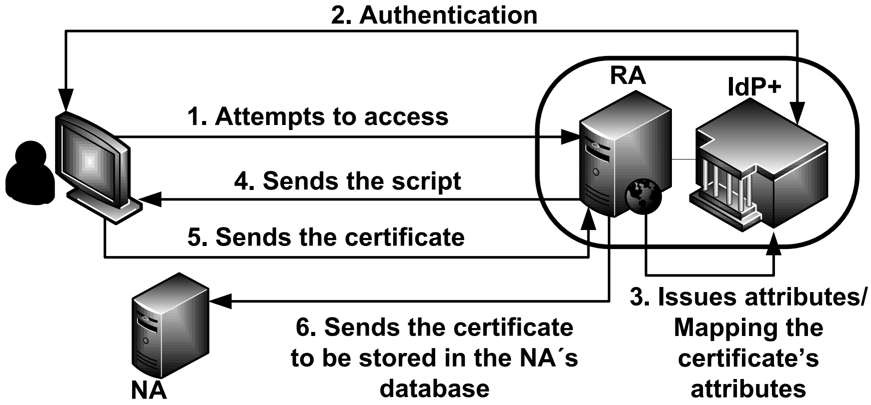

2. Authentication
RA
IdP+
1. Attempts to access
4. Sends the script
5. Sends the certificate
3. Issues attributes/ Mapping the certificate's attributes
6. Sends the certificate to be stored in the NA´s database
NA

Figure 3. Creation of the user self-signed certificate through Shibboleth Federation.

The figure 3 shows the flows for the creation of the user self-signed certificate through the Shibboleth Federation. After a success authentication, RA does the mapping through SAML assertions issued by IdP+ to compose the certificate's *DN* (Distinguished Name). This mapping gets the user's *SN* (surname) plus the *EPPN* (eduPersonPrincipalName) from the EduPerson [Internet2 2011a] LDAP scheme to set the certificate's *CN* (Common Name). Then the RA sends a script to the user via web browser. The keys and the certificate are created at the user system. The user returns his certificate to the RA and it sends to the NA. Now, NA is ready to issues the proof.

One unique proof can be used as many times as needed, without the necessity of getting other information. In the Shibboleth Federation, the use of the certificate and its proof through a desktop application authentication realizes with some changes of the standard IdP structure.

For desktop authenticated application, this new IdP structure (called IdP+) is like in the infrastructure used by the GT-STCFed project. The STS permits to a desktop application communicates to the Shibboleth providers. The user, through the desktop application, does the authentication with his self-signed certificate and the application gets the proof from NA and sends to IdP+.

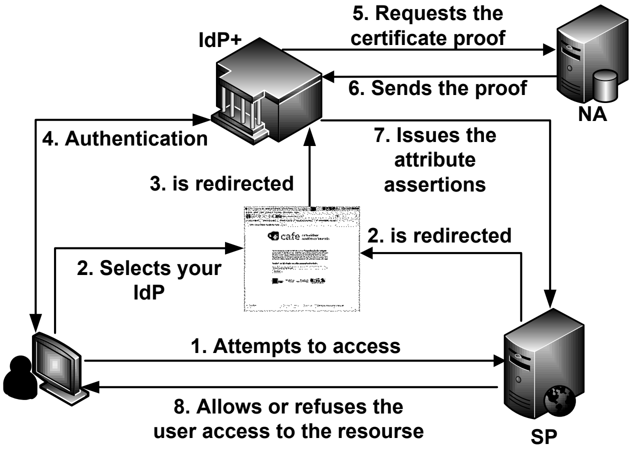

IdP+
5. Requests the certificate proof
6. Sends the proof
NA
4. Authentication
7. Issues the attribute assertions
3. is redirected
2. is redirected
2. Selects your IdP
1. Attempts to access
8. Allows or refuses the user access to the resourse
SP

Figure 4. User authentication with his self-signed certificate and its proof.

The Figure 4 shows the user accessing a service by doing his authentication through the Shibboleth Federation and with his self-signed certificate. If SP provides a web service, then the redirections are needed as a typical Shibboleth Federation, otherwise they do not exist.

5.1. Grid Scenario

In the Grid Scenario, authentication and authorization is based on the use of X.509 certificates, signed by a Certificate Authority. Delegation (a service "A" tries to access service "B" on behalf of the user) is implemented using proxy certificates (short lived, fully functional certificates, that can be traced back to the original user). This PKI system works well for many different applications, including web browsers, but is complex and difficult for many users [Assembla 2011].

The figure 5 shows the flows for a GRID certificate generation that uses self-signed certificates at a Shibboleth environment. The following steps are:

1. The user attempts to access the service that generates the grid certificates.
2. Then the user will be redirected to the WAYF.
3. The user selects his IdP and he is redirected to his institution's log-in site.
4. He does the authentication using his self-signed certificate.
5. IdP+ requests the certificate proof to the NA.
6. IdP+ receives the proof from the NA.
7. If the authentication was concluded, the IdP+ sends the user's information to the SP.
8. The service sends a script to the user to build the certificate's request with his self-signed certificate information and his private key. This request is made at the user's environment and then is sent to the service.
9. The service receives the request, assigns it and then returns the new X.509 certificate.
10. Now the user can use the grid service.

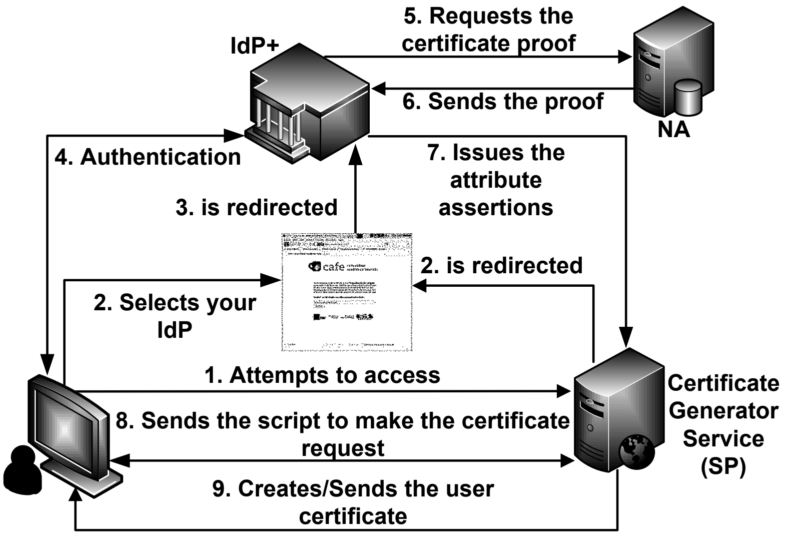

5. Requests the certificate proof
IdP+
6. Sends the proof
NA
4. Authentication
7. Issues the attribute assertions
3. is redirected
2. is redirected
2. Selects your IdP
1. Attempts to access
Certificate Generator Service (SP)
8. Sends the script to make the certificate request
9. Creates/Sends the user certificate

Figure 5. Grid certificate generation.

6. Conclusion and Future Works

This new model of Public Key Infrastructure, NBPKI, provides some facilities for digital signature validation. This model uses self-signed certificates for the users, and the Certificate Authority is replaced by the Notarial Authority. The NA is responsible for the emission of *tokens* which are like a validation proof of the user certificate. With these *tokens*, it is not necessary to verify and validate the certificate chain of the user certificate, to check the certificate revocation lists nor the Time Stamping Authority is necessary.

This new model is useful for improving authentication process in services which use X.509 certificates within an academic federated environment. The Shibboleth Federations can be more usable when have more support to use different authentication credentials.

The use of self-signed certificates improves the facilities of the certificates management, the use of certificates for authentication processes and even the security of the user authentication. The facilities of the issue of digital certificates without losing the infrastructure security and integrating with the academic institutions through Shibboleth Federations, becomes this model one positive different view for the increase of the use of digital certificates for authentication.

The authentication structure does not need to suffer a lot of alterations in the academic federated infrastructure and in the protocols used. The complexity needed by the standard certificate verification may be kept aside whether self-signed certificate is used for the authentication process.

The NBPKI and the IdP+ were implemented in Java language due to be portable and the facility in web applications development. The next stages for the improvement of this work is to perform tests to verify the impacts due to the use of the authentication based on self-signed certificates in the Shibboleth Federations.

References

Al-Riyami, S. and Paterson, K. (2003). Certificateless Public Key Cryptography. *Advances in Cryptology-ASIACRYPT 2003*, pages 1–40.

Assembla (2011). Confusa project. http://www.assembla.com/wiki/show/confusa.

Cantor, S. (2005). Shibboleth architecture - protocols and profiles. Technical report, Internet2. http://shibboleth.internet2.edu/docs/internet2-mace-shibboleth-archprotocols-200509.pdf.

Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and Polk, W. (2008). Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 5280 (Proposed Standard).

de Mello, E., Wangham, M., da Silva Fraga, J., de Camargo, E., and da Silva Böger, D. (2009). A model for authentication credentials translation in service oriented architecture. In Gavrilova, M., Tan, C., and Moreno, E., editors, *Transactions on Computational Science IV*, volume 5430 of *Lecture Notes in Computer Science*, pages 68–86. Springer Berlin / Heidelberg.

Directorate, C. (2011). Cilogon. http://www.cilogon.org/.

Don and Smith (2008). The challenge of federated identity management. *Network Security*, 2008(4):7 – 9.

Ellison, C., Frantz, B., Lampson, B., Rivest, R., Thomas, B., and Ylonen, T. (1999). SPKI Certificate Theory. RFC 2693 (Experimental).

Gentry, C. (2003). Certificate-based encryption and the certificate revocation problem. In *22nd Annual International Conference on the Theory and Applications of Cryptographic Techniques*.

Howlett, J. (2011). Project moonshot. http://www.project-moonshot.org.

Internet2 (2011a). eduperson & eduorg object classes. http://middleware.internet2.edu/eduperson/.

Internet2 (2011b). Incommon. http://www.incommonfederation.org/.

Internet2 (2011c). Internet2. http://www.internet2.edu/.

Internet2 (2011d). Shibboleth. http://shibboleth.internet2.edu/.

Lancaster, S., Yen, D. C., and Huang, S.-M. (2003). Public key infrastructure: a micro and macro analysis. *Computer Standards &amp; Interfaces*, 25(5):437 – 446.

Linn, J. (2004). An Examination of Asserted PKI Issues and Proposed Alternatives. *Proceedings of the 3rd Annual PKI R&D Workshop*.

Moecke, C. T. (2011). Nbpki - uma icp baseada em autoridades notariais. Master's thesis, Universidade Federal de Santa Catarina.

Moecke, C. T., Custódio, R. F., Kohler, J. G., and Carlos, M. C. (2010). Uma ICP baseada em certificados digitais autoassinados. In *Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, pages 91–104, Fortaleza. SBSEG.

OASIS (2011). Oasis - advancing open standards for the information society. http://www.oasis-open.org/.

Rivest, R. L. (1998). Can We Eliminate Certificate Revocations Lists? In *FC '98: Proceedings of the Second International Conference on Financial Cryptography*, pages 178–183, London, UK. Springer-Verlag.

RNP (2011). Cafe. http://www.cafe.rnp.br.

Scavo, T. and Cantor, S. (2005). Shibboleth architecture - technical overview. working draft, Internet2. http://shibboleth.internet2.edu/docs/draft-mace-shibboleth-tech-overview-latest.pdf.

Shamir, A. (1984). Identity-based Cryptosystems and Signature Schemes. In *Advances in Cryptology-Crypto'84*, pages 47–53.

Wangham, M. S., da Silva Fraga, J., and de Mello, E. R. (2011). Gt-stcfed – serviços para transposição de credenciais de autenticação federadas. http://gtstcfed.das.ufsc.br.

Wangham, M. S., de Mello, E. R., da Silva Böger, D., Fraga, J., and Guérios, M. C. (2010). Uma Infraestrutura para Tradução de Credenciais de Autenticação para Federações Shibboleth. In *X Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, pages 360–447, Fortaleza. SBSEG.