Um Conjunto de Requisitos para Políticas de Certificado e Declarações de Práticas de Certificação

Daniel C. Marques, Vinod E. F. Rebello

Instituto de Computação
Universidade Federal Fluminense (UFF) – Niterói, RJ – Brasil
{dmarques, vinod}@ic.uff.br

1. Introdução

Infraestruturas de Chaves Públicas (ICPs) estão se tornando cada vez mais populares por apresentarem uma solução de autenticação flexível, possibilitando a conformidade com requisitos técnicos e legais que exijam a utilização de sistemas com forte esquema de autenticação e que permitam melhor controle sobre a identidade dos usuários. Uma Autoridade Certificadora (AC) age como uma âncora de confiança, estabelecendo uma relação confiável entre as entidades envolvidas em uma transação eletrônica. Contudo, seu gerenciamento apresenta um desafio, pois essa relação transitiva só é possível se houver alguma forma de conhecer a AC o suficiente para que uma opinião seja formada [Lekkas, 2003]. Atualmente, uma AC que deseja emitir certificados digitais fornece aos seus participantes, através das Políticas de Certificado (PC) e da Declaração de Prática de Certificação (DPC), informações sobre políticas e procedimentos para a gestão dos serviços oferecidos por ela. O padrão *de facto* utilizado atualmente para a elaboração desses documentos, a RFC 3647 [Chokani *et al*., 2003], apresenta um arcabouço genérico com o objetivo de apoiar essa atividade, apenas fornecendo uma lista de potenciais tópicos a serem cobertos. Por esse motivo, não oferece critérios a serem considerados pelas entidades confiantes, restando ainda alguma complexidade no trabalho de elaboração de PCs e DPCs e deixando dúvidas sobre o que uma entidade confiante deve exigir de uma AC considerada confiável. O objetivo deste trabalho é estabelecer um conjunto de requisitos que permita o preenchimento das lacunas deixadas pela RFC 3647 através de normas técnicas e padrões reconhecidos e consolidados de segurança e de certificação digital, definindo um conjunto de critérios a serem considerados por autores de PCs e DPCs e entidades confiantes.

2. Política de Certificado e Declaração de Práticas de Certificação

Uma PC é um conjunto de diretivas que define a aplicabilidade de um certificado, provendo informações que permitam ao seu usuário identificar se é apropriado para um uso em particular. Consequentemente, uma AC pode publicar mais de uma PC (ou diferentes políticas em uma única PC), dependendo da aplicação ou tipos de certificados. Uma DPC é um relato das atividades (práticas) exercidas por uma AC para oferecer o serviço de gerenciamento do ciclo de vida de um certificado, isto é, sua emissão, revogação, renovação, re-emissão de chaves e publicação das informações relacionadas a estas. PC e DPC estão fortemente relacionadas. Enquanto a PC determina "o que" deve ser feito, a DPC descreve "como" são executadas as atividades necessárias, podendo constar em um único documento de PC/DPC.

3. Um conjunto de requisitos para PCs e DPCs

Em [Chadwick e Basden, 2001], os autores apresentam alternativas para aquisição do conhecimento necessário para uma avaliação de confiança. Dentre as apresentadas, aqui se utilizou os principais padrões e guias que pudessem suportar os processos de operação e gerenciamento de um serviço de certificação digital, considerando a confiança pré-estabelecida pela comunidade de segurança da informação. A RFC 3647 foi utilizada como modelo para o documento criado, a fim de oferecer um padrão que facilite a comparação entre documentos de PC/DPC e a verificação de conformidade entre os requisitos e os documentos de PC/DPC. Para definição dos requisitos, as seguintes referências foram determinadas relevantes: ISO/IEC 27001:2005 - *Information technology - Security techniques - Information security management systems – Requirements* e ISO/IEC 27002:2005 - *Information technology - Security techniques - Code of Practice for Information Security Management*, que definem requisitos e boas práticas para um Sistema de Gerenciamento de Segurança de Informações; ETSI TS 102 042 - *Policy requirements for certification authorities issuing public key certificates*, que provê um conjunto de requisitos para operação de autoridades certificadoras; e ANSI/X9 X9.79-1:2001 - *Financial Services Public Key Infrastructure (PKI) Policy and Practices Framework* que define os componentes de uma ICP e estabelece requisitos de políticas e práticas relacionadas. A partir destas, foi possível estabelecer requisitos mínimos a serem atendidos por uma AC considerada confiável.

4. Considerações Finais

Este trabalho está sendo aplicado no contexto de uma ICP nacional, através de um conjunto de requisitos mínimos e boas práticas fornecido aos gerentes das ACs. O produto resultante é um importante passo no sentido de facilitar a escrita e avaliação de documentos de PC/DPC, por possibilitar aos autores e às entidades confiantes estabelecer critérios que permitam determinar a confiança em uma AC. É também ponto de partida para o desenvolvimento de soluções para avaliação automática da confiança a partir de PCs e DPCs, como identificado pelo trabalho proposto em [Casola *et al*., 2007]. Futuramente, será estabelecida uma métrica para a avaliação de conformidade dos documentos de PC/DPC com os requisitos propostos e níveis de garantia (*Levels of Assurance - LoA*) pré-definidos.

Referências

Casola, V., Luna, J., Manso, O., Mazzoca, N., Medina, M., Rak, M. (2007), Static evaluation of Certificate Policies for GRID PKIs interoperability, Proceedings of the First International Conference on Availability, Reliability and Security (ARES'07).

Chadwick, D. W. e Basden, A (2001), Evaluating Trust in a Public Key Certification Authority, Computers & Security, 20(7), pg. 592-611.

Chokhani, S., Ford, W., Sabett, R., Merrill, C. e Wu, S. (2003), RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Disponível em: http://www.ietf.org/rfc/rfc3647.txt

Lekkas, D. (2003), Establishing and Managing Trust within the Public Key Infrastructure, Computer Communications, 26(16), 1815-1825.