Relato de Experiência: Adoção de Lista de Serviços de Confiança na Rede Nacional de Ensino e Pesquisa

Nicole Rieckmann[3], Eduardo Perottoni[1], Frederico Schardong[1,2], Lucas Mayr[1], Ricardo Custódio[1], Luciano Rocha[3], Reinaldo Matushima[3]

[1]Laboratório de Segurança em Computação (LabSEC)
Universidade Federal de Santa Catarina (UFSC)

[2]Instituto Federal do Rio Grande do Sul (IFRS)

[3]Rede Nacional de Ensino e Pesquisa (RNP)

Resumo. *Este artigo explora o desenvolvimento e a gestão da Lista de Serviços Confiáveis (LSC), um repositório que armazena informações sobre serviços confiáveis em um documento XML interoperável, pela Rede Nacional de Ensino e Pesquisa (RNP). A LSC desempenha um papel crucial na garantia da segurança e integridade dos serviços digitais, facilitando processos como assinaturas eletrônicas e verificações de autenticidade. A gestão da LSC envolve o cumprimento rigoroso dos requisitos técnicos e de segurança estabelecidos pela ETSI. Este trabalho detalha a estrutura da LSC, e os macroprocessos de inclusão e exclusão de serviços criados pela RNP, destacando sua importância para a confiança dos serviços catalogados.*

1. Introdução

Lançado em março de 2021 o serviço de certificado pessoal da ICPEdu é o serviço de certificação digital oferecido pela Rede Nacional de Ensino e Pesquisa (RNP) que provê infraestrutura para a emissão de certificados digitais que podem ser usados por alunos, professores e servidores de instituições que possuem acesso à Comunidade Acadêmica Federada (CAFe). Entretanto o número de certificados emitidos anualmente vem caindo. No total, foram emitidos 97 147, 63 728, 49 102, e 17 361 certificados anualmente entre 2021 e 2024, respectivamente. Diante desse cenário a RNP realizou uma pesquisa com as instituições que aderiram ao serviço para saber o motivo pelo desinteresse. O resultado da pesquisa deixou claro que a oferta da RNP não contemplava toda a jornada necessária para a assinatura digital de um documento, ou seja, o certificado era entregue ao usuário, mas ele não conseguia efetuar a assinatura sem a utilização de um serviço externo à RNP.

Perante o exposto, a RNP mudou a estratégia e vem modelando um novo serviço que permite ao usuário realizar a jornada inteira, da emissão de certificados digitais, assinatura de documentos, e até a verificação de documentos assinados através de uma plataforma online [Perottoni et al. 2023] focada na experiência do usuário final. Este serviço é o primeiro a utilizar a Lista de Serviços Confiáveis (LSC) da RNP. A LSC, sua estrutura e os processos envolvidos nasceram dentro do escopo do verificador mas evoluíram para um serviço à parte. Neste artigo, apresentamos para a comunidade o conceito de LSC, como ela é usada para gerenciar cadeias de confiança, sua importância para as organizações e relatamos como a gestão da LSC foi implementada dentro da RNP.

2. Background: Lista de Serviços Confiáveis

A Lista de Serviços Confiáveis (LSC) é um documento no formato Extensible Markup Language (XML) que armazena informações de identificação e histórico acerca de provedores de serviços de confiança e seus serviços. A estrutura e sintaxe desse documento são definidas pelo *European Telecommunications Standards Institute* (ETSI) [ETSI TS 119 612 2016]. A Figura 1 ilustra a estrutura de uma LSC.

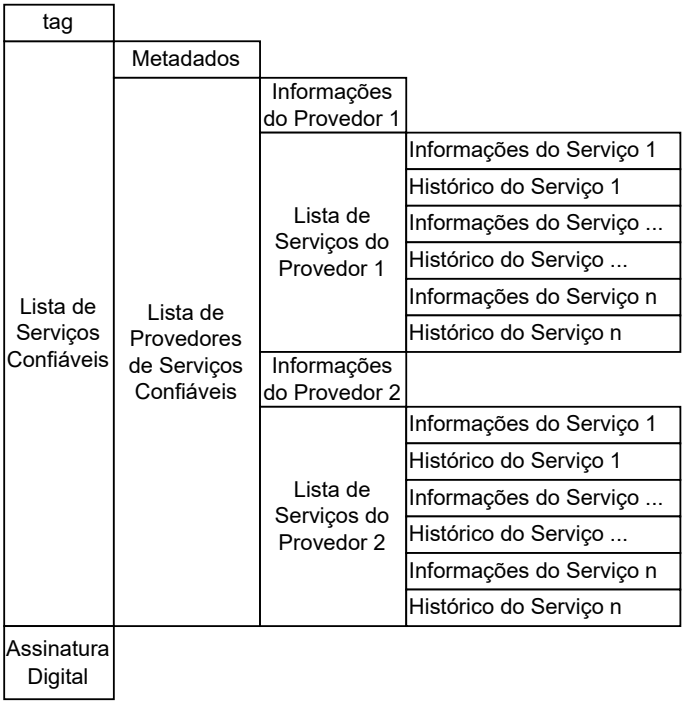

Figura 1. Estrutura da LSC.

A LSC contém metadados acerca da lista e do seu responsável, *i.e.*, o operador da lista. São exemplos de informações contidas na lista: data de emissão e validade, URLs de disponibilidade da lista e nome e endereço do operador. Nota-se também que a LSC contém detalhes de cada entidade que o operador confia. Cada entidade de confiança deve ter pelo menos um serviço confiável, representado por um certificado digital x509, que por sua vez, representa uma âncora de confiança indicando que o operador confia nesse certificado e todos os outros hierarquicamente abaixo dele.

No âmbito da verificação de documentos assinados, um dos requisitos para a validação da assinatura é que, ao reconstruir a cadeia de certificados correspondente ao certificado que assinou o documento, deve-se alcançar uma das âncoras de confiança presentes na LSC. Este processo de reconstrução assegura o rastreamento até uma Autoridade Certificadora (AC) confiável, reforçando a autenticidade e integridade da assinatura.

Além disso, a sintaxe padronizada da LSC viabiliza interoperabilidade entre sistemas distintos, permitindo que interpretem a LSC conforme os padrões estabelecidos pelo ETSI TS 119 612. Ademais, a estrutura da LSC permite apontamentos a outras LSCs, o que possibilita a criação de uma rede de confiança entre organizações. Tal configuração não apenas aprimora os processos de verificação e autenticação de documentos, mas também promove uma colaboração segura entre diferentes plataformas.

3. Gestão da LSC da RNP

Os macroprocessos relacionados com a gestão da LSC da RNP são apresentados na Figura 2. Para implementar a LSC é fundamental entender sua estrutura, evitando assim a descaracterização da LSC e o descrédito dos serviços e provedores listados do operador. Desse modo, para a gestão eficaz da LSC, foram estabelecidos pontos de controle durante as etapas de cada macroprocesso de gestão da LSC.

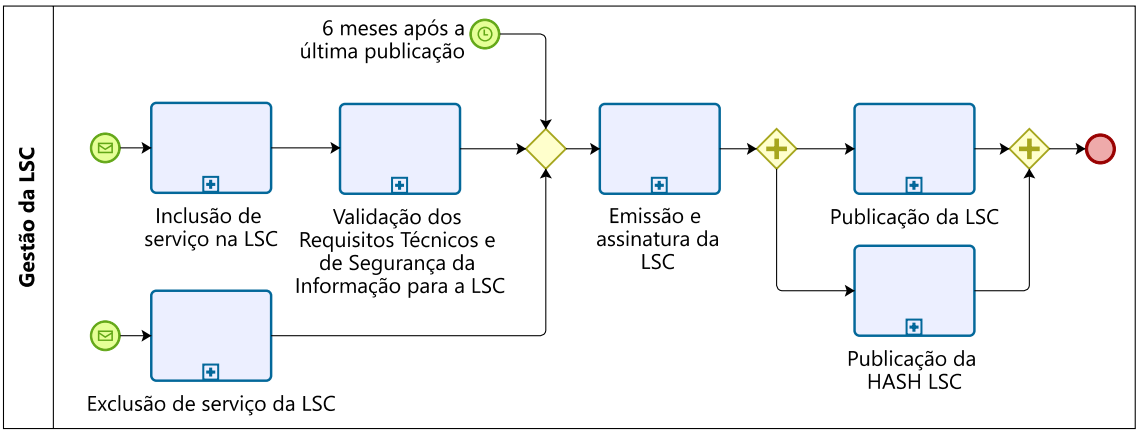

Figura 2. Processo de Gestão da LSC.

Primeiramente, deve-se entender cada elemento da LSC e preenchê-lo conforme os padrões estabelecidos pelo ETSI, atentando-se à sintaxe e campos obrigatórios. Somente então são incluídos os provedores e seus serviços. Cabe considerar, ainda, as regras estabelecidas para garantir a validade da lista, como por exemplo, sua republicação a cada seis meses ou sempre que houver alteração em seus campos obrigatórios.

Como os dados do operador da lista variam esporadicamente, administrar a LSC consiste em gerir os provedores e seus serviços. Nesse contexto, executam-se os processos de inclusão e exclusão dos serviços. A inclusão de novos serviços requer uma validação de requisitos técnicos e de segurança.

Na Figura 3 está esquematizado o processo de inclusão de um serviço na LSC. Esse processo ocorre tanto na inserção de um novo serviço ou na atualização de um já existente, uma vez que a atualização requer a exclusão seguida da inserção do serviço com seus dados vigentes. Entretanto, para inclusão de novos serviços, os setores de Tecnologia da Informação (TI) e Cibersegurança executam as análises pertinentes, a fim de atestar a devida conformidade do serviço acerca de requisitos técnicos e segurança da informação.

Caso o serviço esteja consoante com os pré-requisitos técnicos de segurança, ele estará apto para inclusão na LSC. Cabe às equipes envolvidas estabelecer rotinas para avaliar e validar os parâmetros mandatórios para emitir, assinar e publicar a LSC. Procedimentos para emissão e assinatura da LSC são realizados com auxílio de uma ferramenta disponível publicamente na Internet[1], que verifica e aponta a sintaxe adequada para cada parâmetro da LSC. Tão logo a lista for emitida e assinada, ela deve ser publicada, substituindo sua versão anterior, garantindo assim sua vigência, integridade e confiabilidade.

[1] `https://web.archive.org/web/20240705183349/https://ec.europa.eu/digital-building-blocks/sites/display/TLSO/Trusted+List+Manager+non-EU`

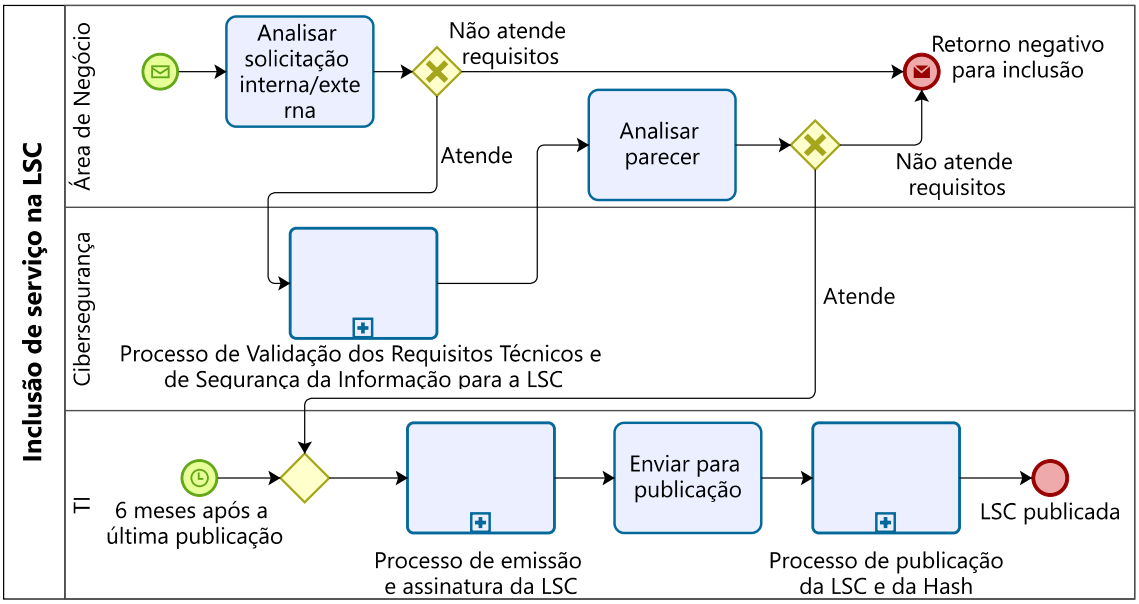

Figura 3. Processo de Inclusão de Serviço na LSC.

4. Conclusão

A adoção da LSC pela RNP é fundamental para garantir a confiabilidade e a segurança dos serviços digitais, especialmente no contexto da plataforma de assinatura e verificação de documentos. A LSC define as âncoras de confiança da organização, assegurando que apenas serviços reconhecidos sejam utilizados por aplicações e parceiros da RNP. A implementação de processos para a gestão da LSC é crucial para manter a integridade e a confiança contínua na lista. Esses processos garantem que a LSC permaneça atualizada, reforçando sua importância como um elemento central na estrutura de confiança da RNP.

Ao integrar a gestão madura da LSC com a plataforma de assinatura digital, a RNP não apenas fortalece a segurança e a confiabilidade dos serviços, mas também cria uma base sólida para o aumento da adoção de assinaturas digitais entre os membros da CAFe. Essa abordagem tem o potencial de aumentar significativamente o uso de certificados ICPEdu, promovendo uma adoção mais consistente e confiável das assinaturas digitais.

Por fim, serão incluídas na LSC raízes de confiança consolidadas no país como a ICP-BR e o gov.br, garantindo interoperabilidade com outros ecossistemas também consolidados nacionalmente. Também está no escopo do projeto a inclusão de raízes de confiança de ensino e pesquisa internacionais, em um esforço maior de reconhecimento mútuo de assinaturas digitais.

Referências

ETSI TS 119 612 (2016). Electronic signatures and infrastructures (esi); trusted lists. Standard, European Telecommunications Standards Institute.

Perottoni, E. D., Costa, B. P., Müller, F. L., dos Santos Camargo, V., Schardong, F., Silvano, W., Mayr, L., Custódio, R. F., Rocha, L., Lyra, C., et al. (2023). Menos certificação digital e mais identidade eletrônica: Icpedu e cafe em um assinador digital inclusivo. In *Anais Estendidos do XXIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, pages 93–96. SBC.