CAFe

Comunidade Acadêmica Federada

Declaração de Práticas de Registro de Metadados

Autores	Laerte F. Belotto, Luciano Rocha e Rui Ribeiro
Data da publicação	30/10/2020
Versão	1.0

Indice

1. Definições e Terminologia

As palavras-chave “DEVE“, “NÃO DEVE“, “REQUER“, “DEVERIA“, “NÃO DEVERIA“, “PODERIA“, “NÃO PODERIA“, “RECOMENDÁVEL“, “PODE“, e “OPCIONAL”, bem como suas correspondentes flexões de número, neste documento devem ser interpretadas como descritas no RFC 2119 [RFC2119] que é livremente traduzido a seguir:

1. DEVE – Esta palavra, ou os termos “REQUER” ou “DEVERIA“, significa que a definição é uma exigência absoluta da especificação.

2. NÃO DEVE – Esta frase, ou a frase “NÃO DEVERIA“, significa que a definição é uma proibição absoluta da especificação.

3. PODERIA – Esta palavra, ou o adjetivo “RECOMENDÁVEL” significa que podem existir razões válidas em circunstâncias particulares para ignorar um item específico, mas todas as implicações devem ser compreendidas e cuidadosamente ponderadas antes de escolher um curso diferente.

4. NÃO PODERIA – Esta frase, ou a frase “NÃO RECOMENDÁVEL“, significa que podem existir razões válidas em circunstâncias particulares em que um comportamento é aceitável ou mesmo útil, mas todas as implicações devem ser compreendidas e cuidadosamente ponderadas antes de implementar qualquer comportamento descrito com essa rotulagem.

5. PODE – Esta palavra, ou o adjetivo “OPCIONAL“, significa que um item é realmente opcional. Um fornecedor pode optar por incluir o item porque um mercado em particular o requer ou porque o fornecedor sente que isso melhora o produto enquanto outro fornecedor pode omitir o mesmo item. Uma implementação que não incluir esta opção em particular DEVE estar preparada para interoperar com outra aplicação que incluir a opção, embora possivelmente com funcionalidade reduzida. No mesmo sentido, uma implementação que inclui a opção em particular DEVE estar preparada para interoperar com outra implementação que não inclui a opção (exceto, é claro, para funcionalidade que a opção fornece).

As seguintes definições são usadas nesse documento:

Federação	Federação de Identidade. Uma associação de organizações que se reúnem para trocar informações de maneira segura sobre seus usuários e recursos, com a finalidade de permitir colaborações e transações.
Membro da Federação	Uma organização que aderiu à Federação por concordar e se comprometer formalmente com as Políticas da Federação.
Operador da Federação	Organização que provê a infraestrutura para Autenticação e Autorização para o Membros da Federação. No contexto da CAFe a RNP desempenha esse papel.
Política da Federação	Documento que descreve as obrigações, direitos e expectativas em relação aos Membros da Federação e ao Operador da Federação
Entidade	Um componente discreto que um Membro da Federação deseja registrar e descrever no metadado. Em geral é um Provedor de Identidade (IdP) ou Provedor de Serviço (SP).
Gerenciador de Metadados	Sistema utilizado pelo Operador da Federação para registrar os metadados da entidades.
Contatos Registrados	Pessoas autorizadas a representar os membros da federação. Podem possuir diferentes papéis com diferentes atribuições.

2. Introdução e Aplicabilidade

Este documento descreve as práticas de registro de metadados do Operador da Federação e tem efeito a partir da data da publicação que consta na capa. Todos os novos registros de entidades realizados após a publicação DEVEM ser analisados conforme aqui descrito até que o documento seja substituído.

Este documento DEVE ser publicado no website da Federação em: https://svn.cafe.rnp.br/repos/CAFe/termos_politicas_CAFe/mrps.pdf. Atualizações documentais DEVEM ser refletidas com precisão nos metadados da entidade.

Uma entidade que não inclua uma referência a uma política de registro DEVE ser assumida como tendo sido registrada sob práticas de registro não documentadas. Solicitações para reavaliar uma determinada entidade a luz deste documento PODEM ser feitas para o Service Desk da RNP.

3. Elegibilidade e Validação de Membros da Federação

Os Membros da Federação são elegíveis para solicitar ao Operador da Federação o registro de entidades. Solicitações provenientes de outras origens NÃO DEVEM ser aceitas.

O procedimento supra tem a finalidade de verificar se o potencial Membro da Federação atende aos requisitos legais existentes e requer o estabelecimento de relação contratual com o Operador da Federação. O Operador da Federação faz verificações com base na razão social fornecida. As verificações podem ser realizadas com base em documentos, bancos de dados públicos e registros próprios.

Durante o procedimento ocorre a identificação e verificação dos Contatos Registrados que possuem a prerrogativa de atuarem em nome da organização para tratativas junto ao Operador da Federação. A verificação é feita por documento emitido pelo dirigente máximo da organização em favor dos Contatos Registrados.

O procedimento ainda estabelece o nome canônico para o Membro da Federação. Tal atributo PODE ser alterado a qualquer momento mediante justificada necessidade. O nome canônico é divulgado no elemento *SAML v2.0 <md:OrganizationName>* da entidade [SAML-Metadata-OS].

4. Formato do Metadado

Todas as entidades DEVERÃO fazer uso da extensão de metadados [SAML-Metadata-RPI-V1.0] para indicar que o Operador da Federação é o registrador da entidade bem como detalhar a versão da DPRM adotada. Exemplo:

```
<mdrpi:RegistrationInfo
registrationAuthority="http://www.rnp.br"
registrationInstant="2020-10-30T15:00:00Z">
<mdrpi:RegistrationPolicy
xml:lang="pt-br">https://svn.cafe.rnp.br/repos/CAFe/termos_politicas_CAFe/mrps
.pdf</mdrpi:RegistrationPolicy>
</mdrpi:RegistrationInfo>
```

5. Elegibilidade e Validação de Entidades

5.1 Registro de Entidade

O Operador da Federação DEVE verificar se um Membro da Federação possui o direito de uso em relação a um nome de domínio relacionado ao entityID e, para Provedores de Identidade, qualquer atributo de escopo.

O direito de uso de um nome de domínio DEVE ser estabelecido de uma das seguintes formas:

- O nome canônico do Membro da Federação corresponde às informações mostradas no WHOIS.
- O Membro da Federação PODE possuir uma autorização formal de uso, específica para uma determinada entidade, emitida pelo proprietário do nome de domínio.

5.2 Formato do *entityID*

Valores para o atributo entityID DEVEM ser uma URI absoluta que use um dos seguintes esquemas: http, https ou urn.

O uso do esquema https é RECOMENDADO a todos Membros da Federação.

Ao usar os esquema http ou https o valor da URI DEVE conter o nome da estação acrescido do nome de domínio. Exemplo: https://estacao.instituicao.br/.

5.3 Formato do escopo

O escopo de entidades do tipo Provedor de Identidade DEVE corresponder ao nome de domínio DNS. São aceitos múltiplos escopos. Expressões regulares NÃO DEVEM ser utilizadas.

5.4 Validação de Entidade

Durante o registro de uma entidade, o Operador da Federação DEVE realizar verificações de validação da entidade. Essas verificações incluem:

- Garantir que todas informações requeridas estão presentes no metadado;
- Garantir que o metadado está bem formado;
- Garantir que os *endpoints* estão corretamente protegidos por certificados TLS/SSL.

6. Gerenciamento de Entidade

Dado que um membro ingressa na Federação qualquer número de entidades PODEM ser adicionadas, modificadas ou removidas pela organização. Em geral cada membro possui apenas um Provedor de Identidade.

6.1 Solicitações de Mudança de Entidade

Todas as solicitações de adição, mudança ou remoção de entidades provenientes de Membros da Federação devem ser feitas através dos Contatos Registrados.

A comunicação de mudança deve ocorrer através do e-mail sd@rnp.br

6.2 Mudança de Entidade Não Solicitadas

O Operador da Federação pode corrigir ou modificar o metadado da Federação a qualquer tempo a fim de:

- Garantir a segurança e integridade do metadado;
- Obter conformidade com acordos firmados com outras Federações ou Confederações;
- Melhorar interoperabilidade;
- Adicionar valor ao metadado.

Mudanças serão comunicadas aos Contatos Registrados da entidade.

7. Referências

[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
[SAML-Metadata-RPI-V1.0]	SAML V2.0 Metadata Extensions for Registration and Publication Information Version 1.0. 03 April 2012. OASIS Committee Specification 01. http://docs.oasis-open.org/security/saml/Post2.0/saml-metadata-rpi/v1.0/cs01/saml-metadata-rpi-v1.0-cs01.html.
[SAML-Metadata-OS]	OASIS Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0: http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf.

8. Atribuição

Este documento foi desenvolvido com base no *REFEDS Metadata Registration Practice Statement template v1.1*.