

CT-GID

Da Identidade Autossoberana à Identidade Fiduciária: Uma Jornada Rumo a Maior Privacidade e Usabilidade do Usuário

Frederico Schardong

Instituto Federal do Rio Grande do Sul (IFRS)

Ricardo Custódio

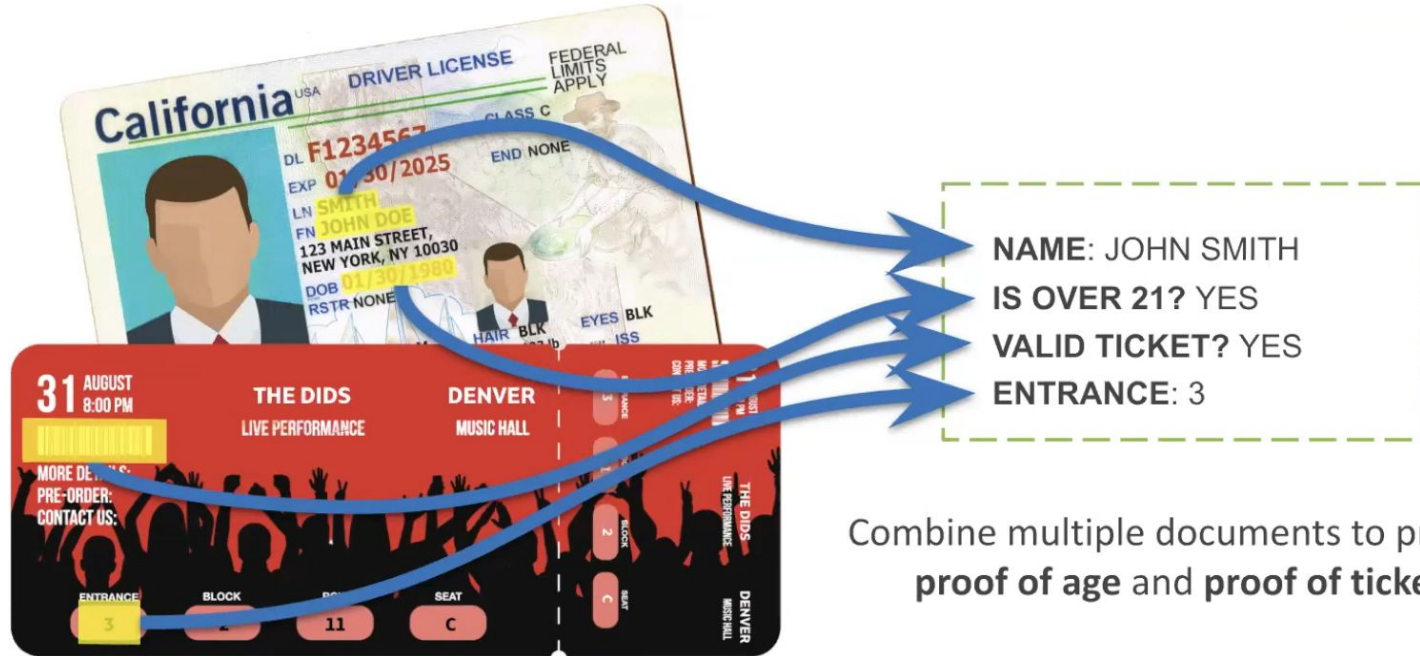
Universidade Federal de Santa Catarina (UFSC)

Identidade Autossoberana

Self-Sovereign Identity (SSI) [7] é um modelo de identidade digital que:

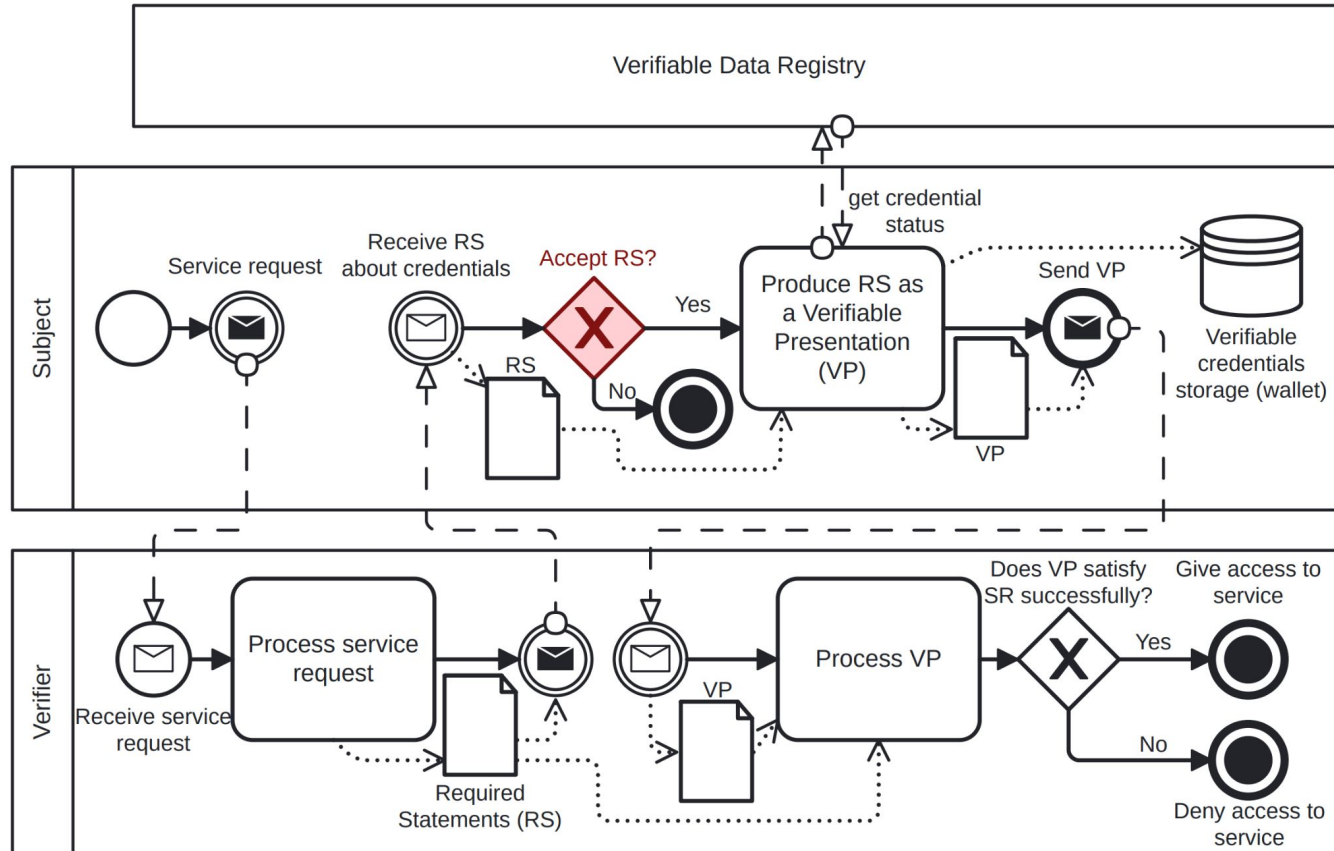
- Pessoas gerenciam suas informações pessoais (credenciais);
- Apresentação de credencial minimiza vazamento de informação;
- IdPs não sabem como/onde as credenciais são usadas.

Identidade Autossobrerana



Combine multiple documents to present
proof of age and **proof of ticket**.

Identidade Autossobrerana



SSI: Desafios em Aberto

- Definição de SSI que pesquisadores e *stakeholders* aceitem;
- Pesquisa básica/fundamental;
- Compartilhamento de atributos não triviais;
- Modelos de confiança robustos;
- SSI sem *blockchain*;
- Migração de outros paradigmas para SSI;
- **Usabilidade.**

SSI: Open Challenges

- Usabilidade:
 - Falta de gestão de consentimento focada no ser humano;



Welcome

 75451442@qq.com

storage.com wants to



View and manage the files in your Google Drive



View and manage Google Drive files and folders that you have opened or created with this app



View the activity history of your Google apps



Allow storage.com to do this?

By clicking Allow, you allow this app to use your information in accordance with their terms of service and privacy policies. You can remove this or any other app connected to your account in [My Account](#)

CANCEL

ALLOW



Instagram is requesting permission to do the following:



Access my basic information

Includes name, profile picture, gender, networks, user ID, list of friends, and any other information I've made public.



Post to Facebook as me

Instagram may post status messages, notes, photos, and videos on my behalf



Access my data any time

Instagram may access my data when I'm not using the application

[Report App](#)

Logged in as Ngoan Nguyen · [Log Out](#)

Don't Allow

Allow

▼ Verifiable Presentation Request

Request Name:

Vaccine Attestation

DID Relationship:

XRK2vHvhqJuUF3ua7tWPKM

Attributes to Selective Disclosure:

+

-

Laboratory

▼

Pathogen

▼

Proof Predicate:

+

-

Attribute:

Dose

▼

Type:

Greater than or equal to

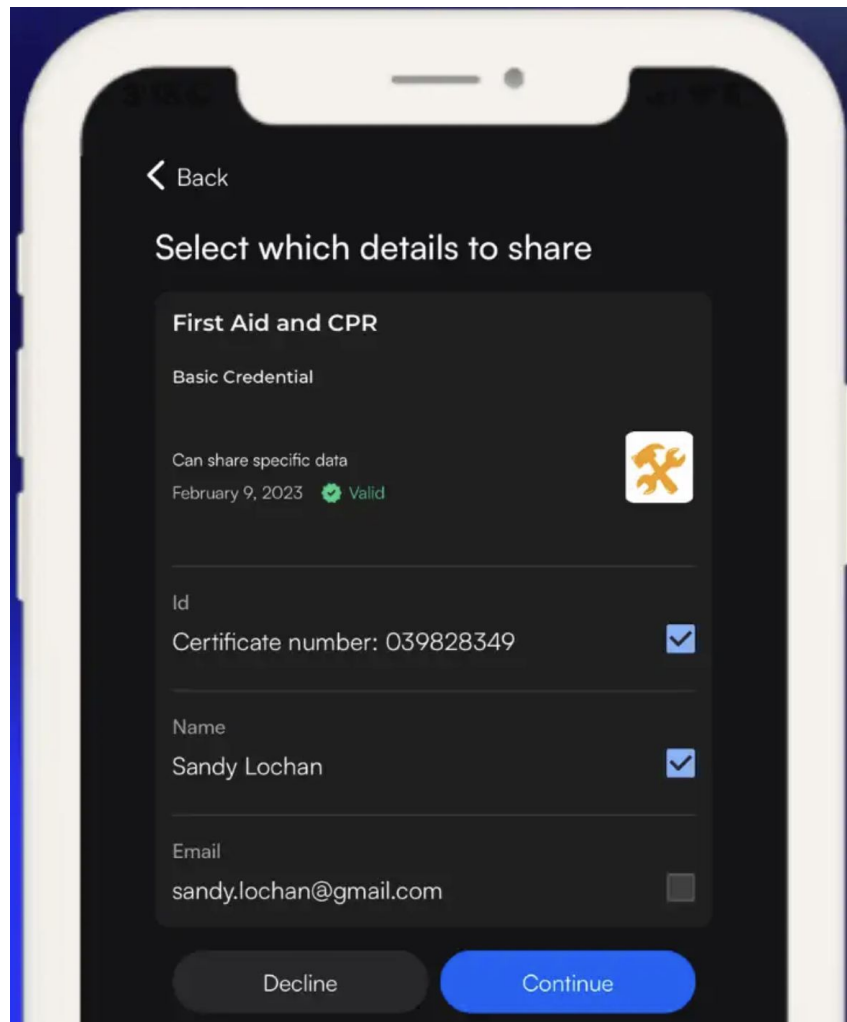
▼

Value:

1

▼

Send Presentation Request



Motivação

- O consentimento é um aspecto central da experiência do usuário online;

Motivação

- O consentimento é um aspecto central da experiência do usuário online;
- Como melhorar a experiência do usuário?

Motivação

- O consentimento é um aspecto central da experiência do usuário online;
- Como melhorar a experiência do usuário?
 - Delegue a tomada de decisões chatas;
 - Automatize decisões de consentimento.

Proposta

- Abraçar a **Relação Fiduciária**;

Proposta

- Abraçar a **Relação Fiduciária**;
 - "Uma parte assume uma posição de autoridade e responsabilidade sobre a outra, exigindo o máximo cuidado, lealdade e transparência.";

Proposta

- Abraçar a **Relação Fiduciária**;
 - "Uma parte assume uma posição de autoridade e responsabilidade sobre a outra, exigindo o máximo cuidado, lealdade e transparência.";
 - "O fiduciário deve priorizar os melhores interesses do beneficiário.";

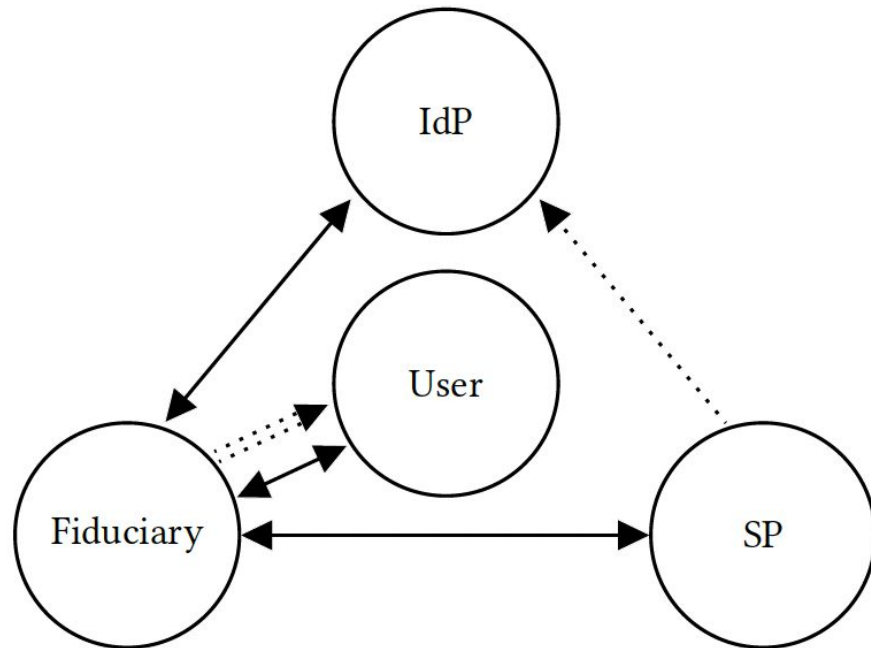
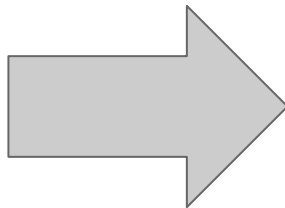
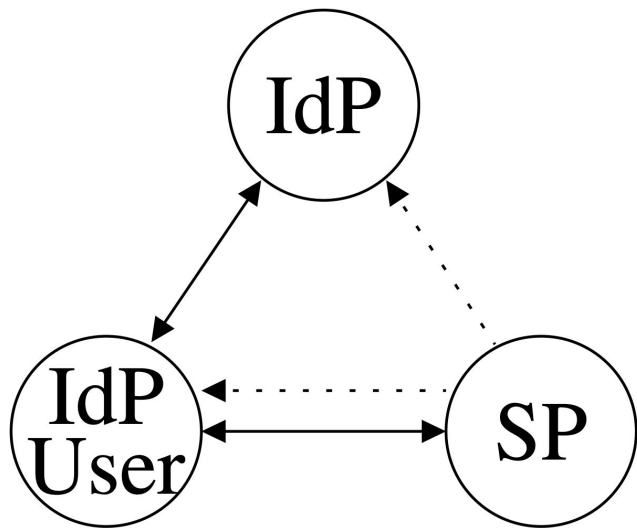
Proposta

- Abraçar a **Relação Fiduciária**;
 - "Uma parte assume uma posição de autoridade e responsabilidade sobre a outra, exigindo o máximo cuidado, lealdade e transparência.";
 - "O fiduciário deve priorizar os melhores interesses do beneficiário.";
 - "O fiduciário ganha poder e superioridade sobre o beneficiário.";

Proposta

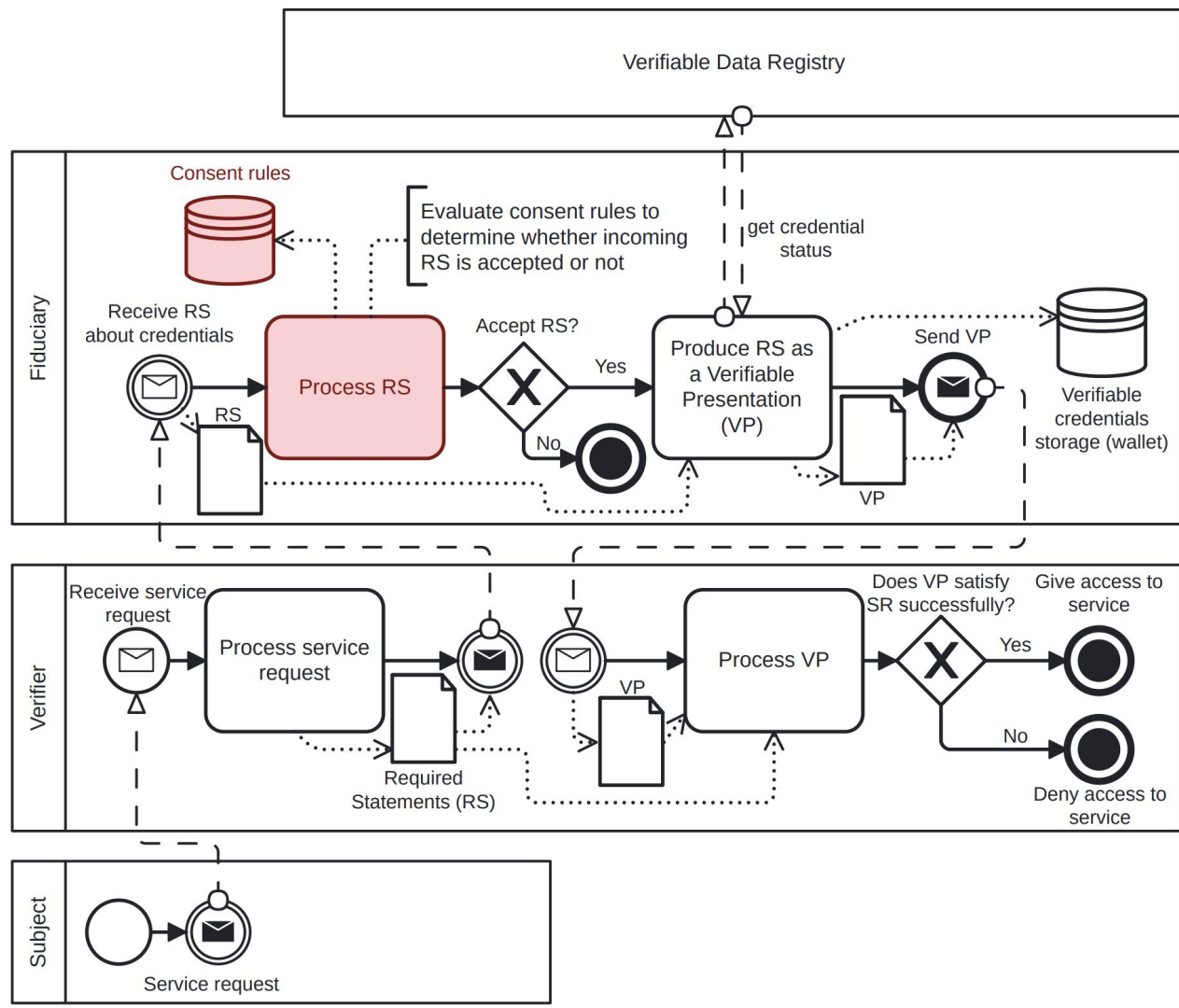
- Abraçar a **Relação Fiduciária**;
 - "Uma parte assume uma posição de autoridade e responsabilidade sobre a outra, exigindo o máximo cuidado, lealdade e transparência.";
 - "O fiduciário deve priorizar os melhores interesses do beneficiário.";
 - "O fiduciário ganha poder e superioridade sobre o beneficiário.";
- Por exemplo:
 - Relação médico e paciente;
 - Relação advogado e cliente.

Proposta



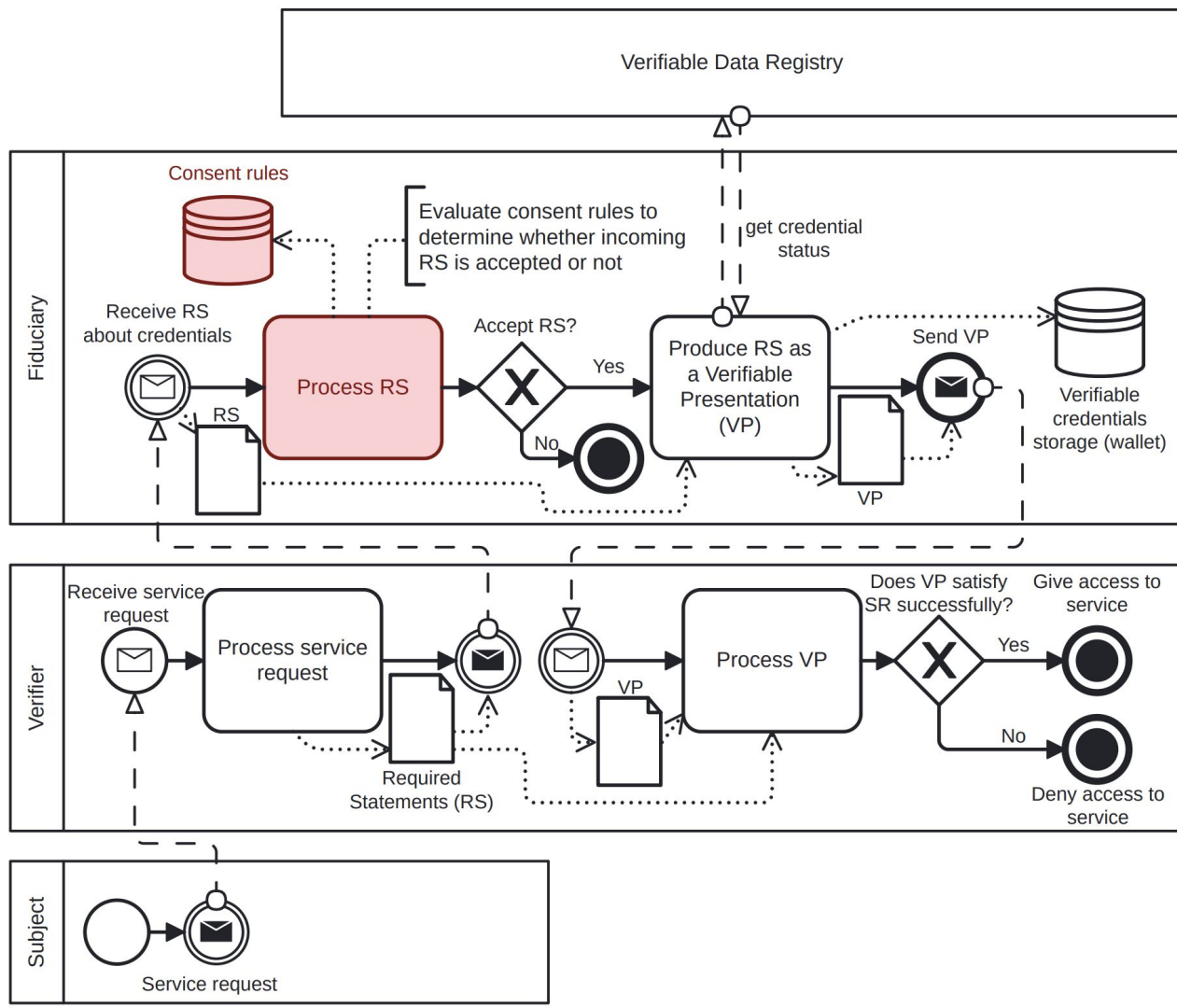
Proposta

- Fiduciário representa o usuário;



Proposta

- Fiduciário representa o usuário;
- Usuário não é importunado;



Proposta

Table 2: Comparison between the main characteristics of the digital identity models.

IAM Model	Decentralization Level	Driving Relationship	Usability Cognitive Load	Private Data Manager	Consent Management	Compute Site
Centralized Outsourced IdP SSI	low	dependence	medium	SP	none	SP
	medium	trust	low	IdP	on demand	SP
	high	trust	high	subject	on demand	SP
Fiduciary Identity	high	fiduciary	low	fiduciary	a priori; on demand; or a posterior	SP; fiduciary; or both

Limitações

- Protocolos devem ser criados para especificar interações;

Limitações

- Protocolos devem ser criados para especificar interações;
- Como expressar consentimento a um fiduciário?

Limitações

- Protocolos devem ser criados para especificar interações;
- Como expressar consentimento a um fiduciário?
- O Modelo de Identidade Fiduciária precisa ser instanciado.

Discussões

- As carteiras digitais em SSI, não são fiduciários?
- Se o fiduciário faz algo errado, quem é o culpado?

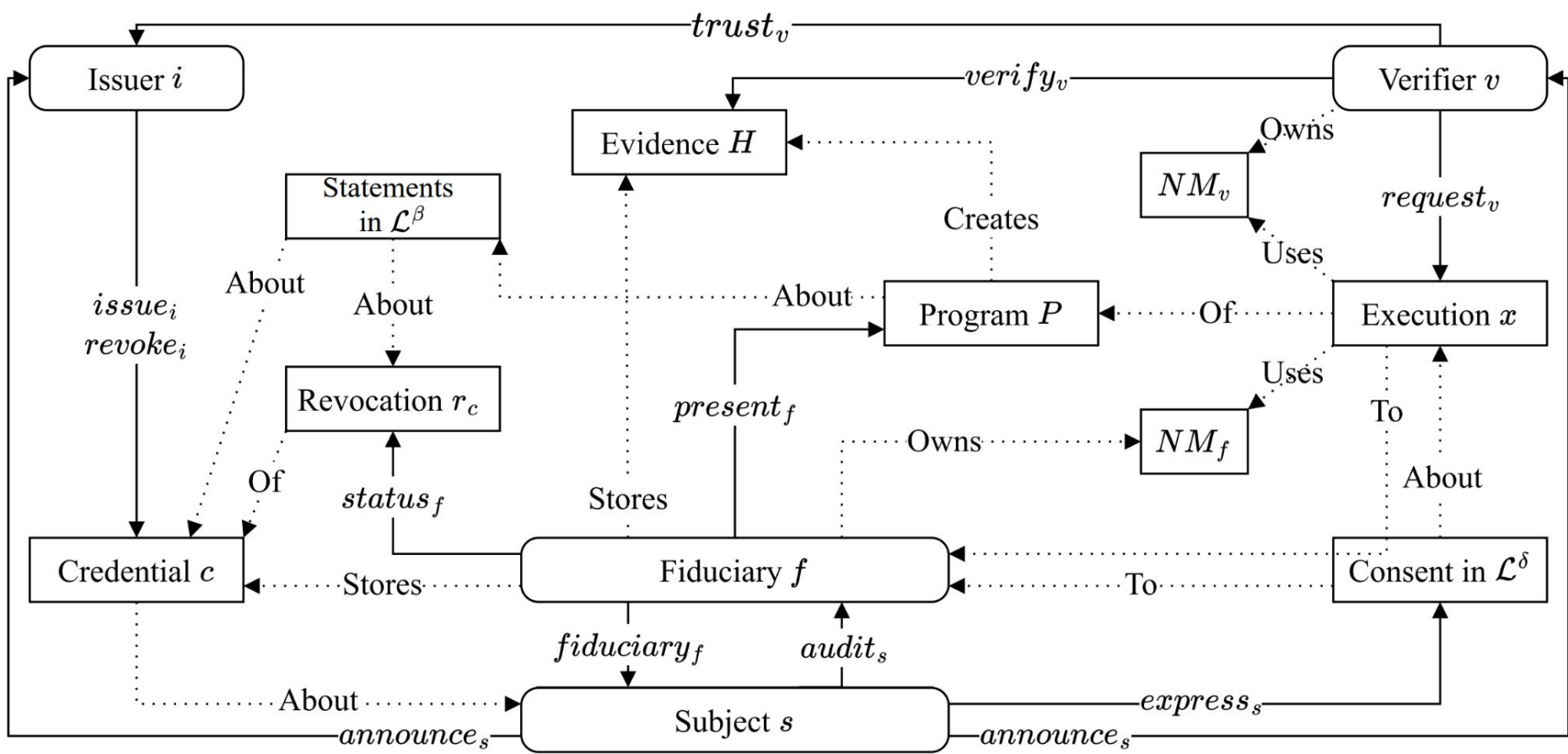
Conclusão

- A relação fiduciária deve ser adotada pelas carteiras digitais;
- O modelo de identidade fiduciária reduz a carga cognitiva dos usuários.

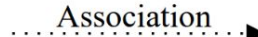
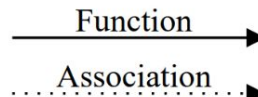
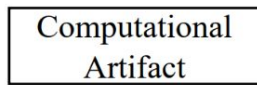
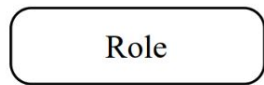
Obrigado!

Perguntas?

Supplementary Material



Caption



What is digital identity?

What is digital identity?

“A digital identity is a **representation** of an entity in a specific context” [4]

[4] ISO, IT Security and Privacy - A framework for identity management
Part 1: Terminology and concepts, Standard, International
Organization for Standardization, Geneva, CH, March 2019.

What is digital identity?

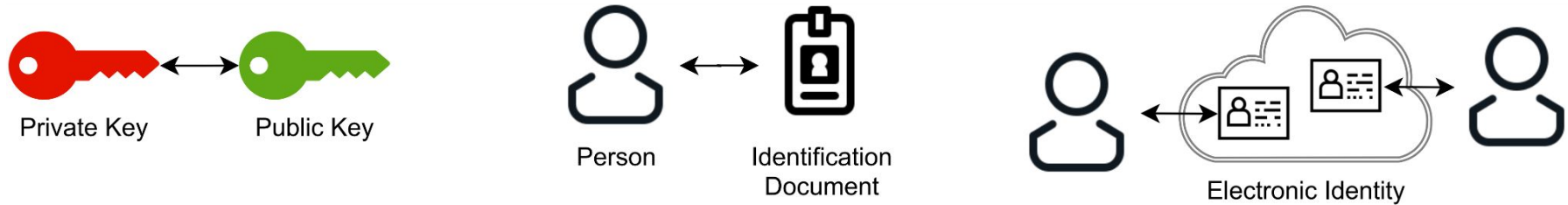
“A digital identity is a **representation** of an entity in a specific context” [4]

“A set of attributes **related** to an entity” [5]

[5] Teruko Miyata et al., A survey on identity management protocols and standards, IEICE TRANSACTIONS on Information and Systems 89 (2006), no. 1, 112–123.

What is identity?

Identity is a relation of **uniqueness** between two entities in a given context



Composition of a Digital Identity

Digital Identity

Identifiers

- Passport Number
- Email Address

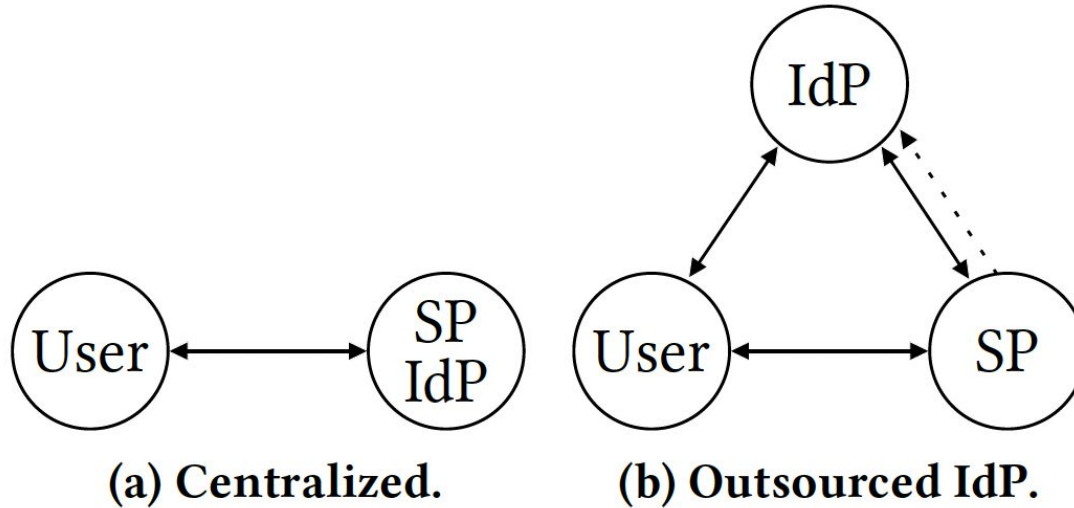
Access Credentials

- Password
- OTP

Other Attributes

- Cell Phone Number
- Name
- Birthdate
- ...

The Evolution of Digital Identity Models



Limitations of Current Models

Lack of freedom $\mapsto$ online existence should be independent of identity providers

Limitations of Current Models

Lack of freedom $\mapsto$ online existence should be independent of identity providers

Lack of autonomy $\mapsto$ people need to be the controller of their attributes

Limitations of Current Models

Lack of freedom $\mapsto$ online existence should be independent of identity providers

Lack of autonomy $\mapsto$ people need to be the controller of their attributes

Lack of privacy $\mapsto$ people's activity should not be monitored

Self-Sovereign Identity

