Attraction Pass - What allows Bob to trust an Attraction Pass Sales Agent?

Thumbnail

Trustable ecosystems will need to support existing and future approaches to ensuring that Parties interaction within (and between) an ecosystem can trust that any component, service or Party is valid and is “who they say they are”. Selling attraction event tickets to consumers has some good examples of trust-problems which are used here to explore various trust approaches across a draft mental model of some of the relationships in the Attraction Pass WG discussions.

Problem Statement

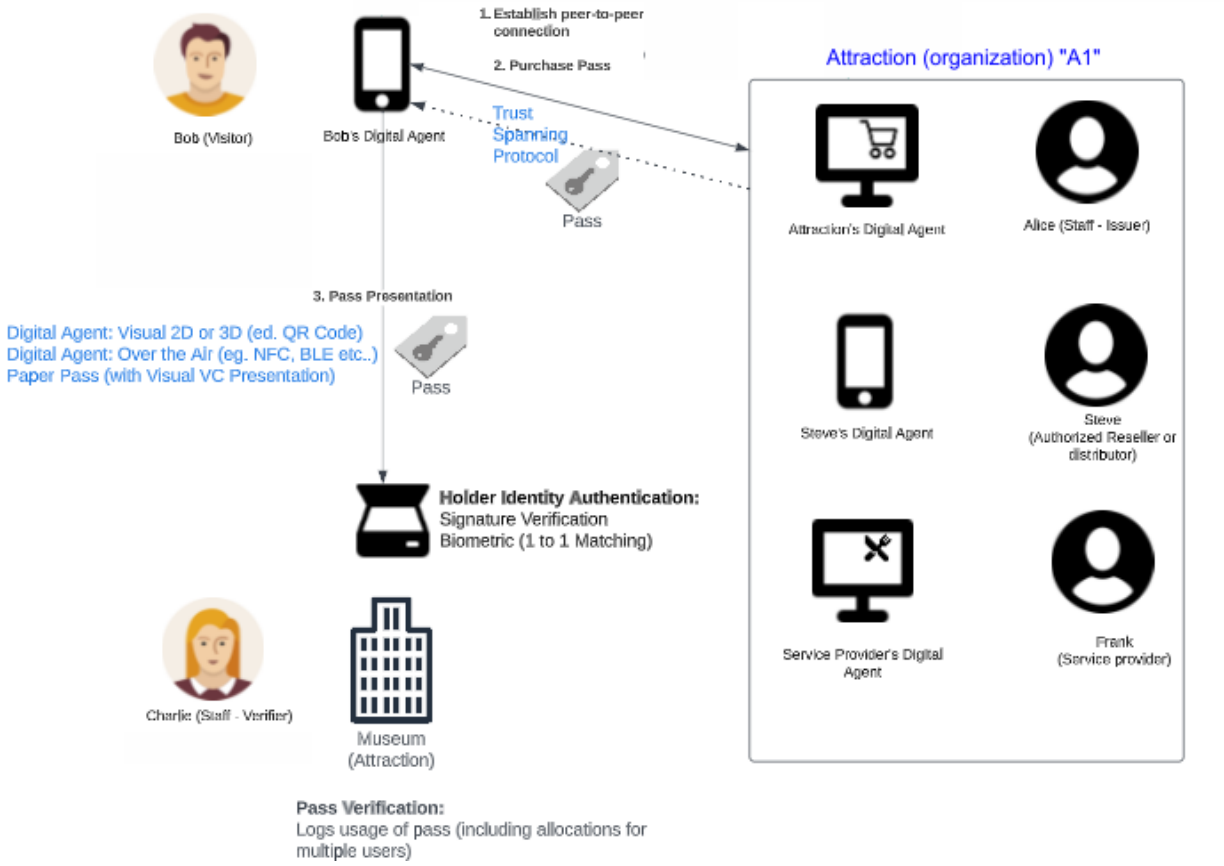
There are several problems with event ticket buying and selling:

1. The buyer needs to know that
    - A sales agent is a verifiable agent of an attraction pass organization
    - That the attraction pass organization is authorized to sell passes for the event.
2. The Attraction Pass Collector (and Attraction event venue management organization) needs to know that:
    - The consumer presenting an Attraction Pass is the legitimate Holder of the Pass (or Passes, in the case of a group for which the consumer holds passes for multiple people)
    - On processing the pass, that the collection system will not allow the pass to be reused (for a single event pass), in any form (on a smartphone or paper).

This draft of this document will cover case 1) what allows Bob to trust an Attraction Pass organization and their authorized Sales Agent Services & Personnel

Current Attraction Pass Model

The following model has been simplified to allow overlay of this document's version of trust mechanisms to address the Problem statement



Narrative

Bob uses his Digital Agent (phone) to connect to the Attraction's Digital Agent to purchase a pass, which is operated by Alice, an "A1" staff member. Bob interacts with the Agent/Staffer and obtains a Museum Pass, which is placed in Bob's Agent's wallet.

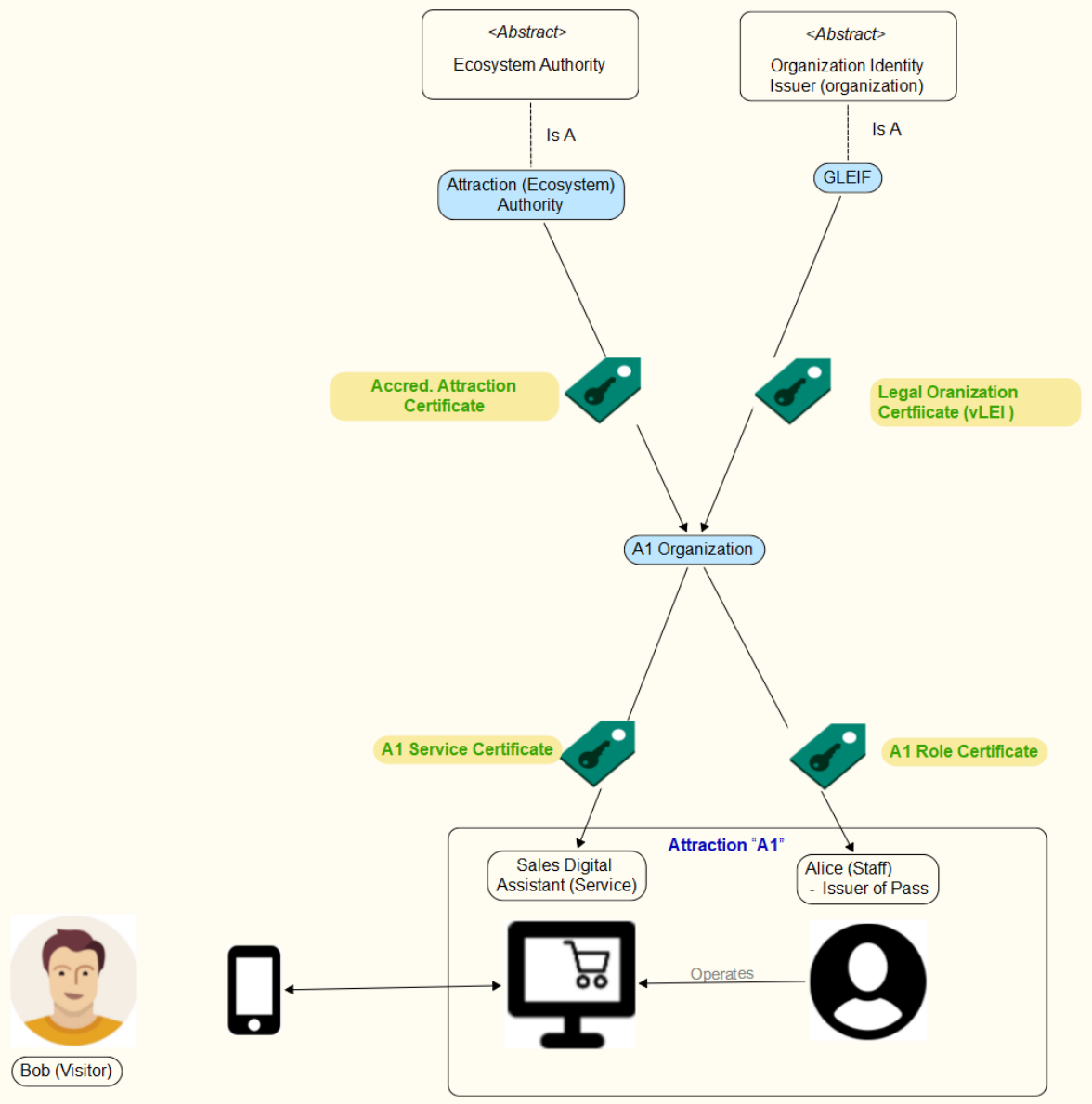
Bob then interacts with Charlie (a staff member who accepts passes (Verifier)) for the event, presenting the Pass (from his Wallet) to Charlie, such that Charlie/her Digital Agent accepts the Pass, which the Attraction "infrastructure" (beyond the scope of this document) to verify this Pass is bound to Bob and has not been previously spent/used.

(Assumption) A mechanisms TBD, marks the Pass Bob presented as "spent/used" both for storage in his wallet and from an event perspective (such that any other presentation of the same Pass by Bob or someone else, will fail.

Bob Trusts A1, it's Services and Personnel - a Certificate view

> Note: Oversimplified view. The relationship between oranization/authorities and Issuers as separate "agents" for the issuance of certificates is not shown to simplify the diagram

Discussions have outlined the following trust paths that Bob will need in order to trust that buying a Pass online via an A1 Sales Digital Assistant, with assistance from Alice



Establish **A1** as accredited **Attraction Pass Seller** for the jurisdiction of the event

- The **Attraction "A1"** organization needs to be a **legimate/legal organization** in the relevant jurisdiction in order to be considered as an **Attraction Pass Seller** under the authority of the **Attraction Ecosystem**.

    - For example purposes, we'll use GLEIF as a recognized Organization Identity Issuer (organization can include an incorporated individual) who can provide such a legal organization certificate.
- The **Attraction Ecosystem** needs to issue an **Attraction Accreditation Certificate** to **"A1"**

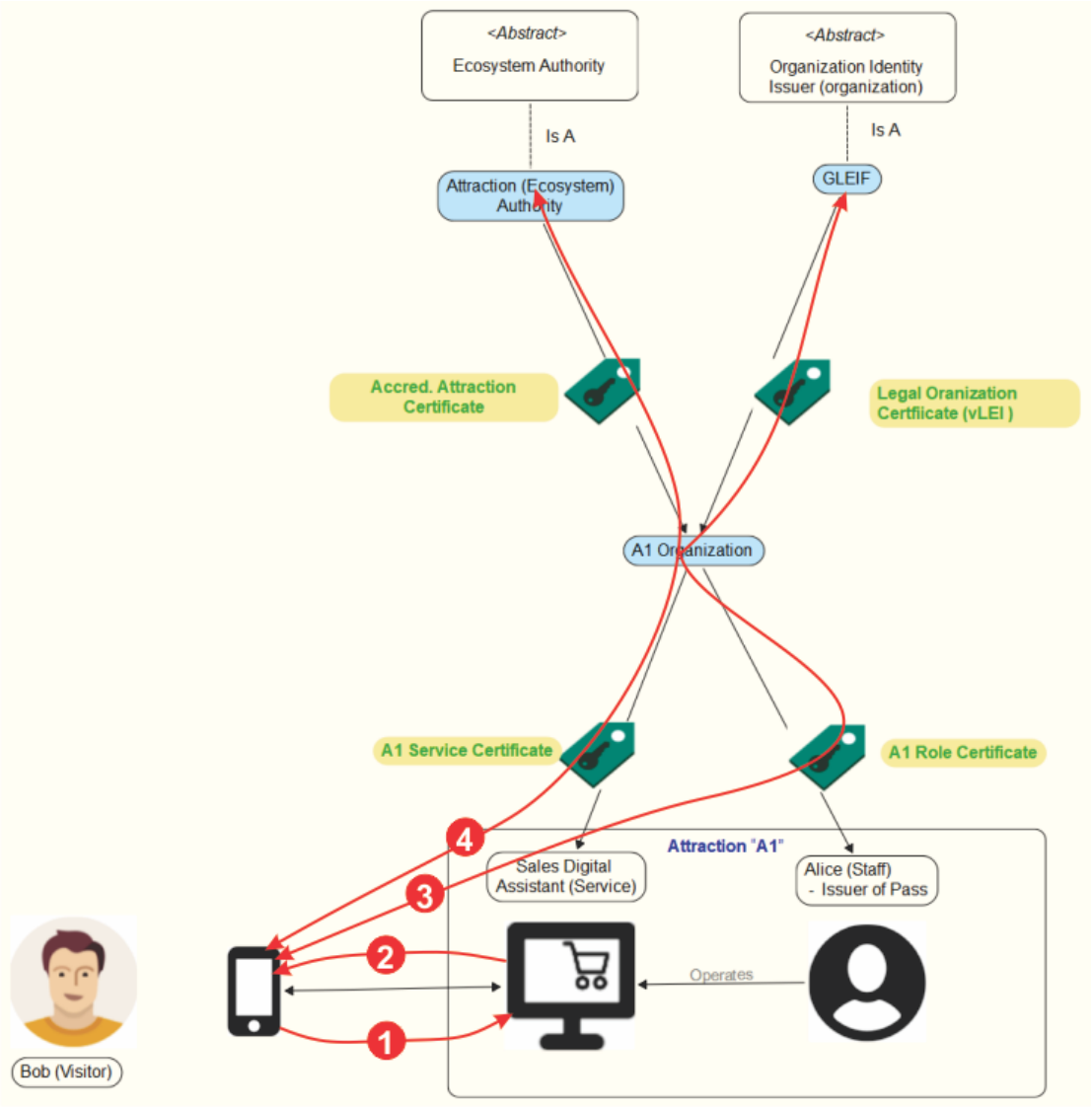
  Note: It is suggested that **"Legal" Organization/Entity Identity Organizations (OEIO)** (and their role as an **Issuer**) needs further discussion. OEIO's may be jurisdiction independent organizations or they may be part of an Ecosystem. It is suggested that the reality will be that Ecosystems will have to have a list of OEIO's identities they accept, even if they have their own, independent OEIO.

A1 needs to establish their **Sales Digital Assistant service** (web site, application, etc.) and **Alice**, as part of the A1 personnel/staff, as a verifiable **Sales Agent**.

- Using the GLEIF conceptual model that a legal organization can designate (with the appropriate governance) Services and Personnel as valid in their Roles for their purposes, a certificate is issued by **A1** to the **Sales Digital Assistant** (as a Service) and to **Alice** (as a person acting in the Role) of a **seller (issuer) of Attraction Passes**.
    - Working assumption: Bob would normally be able to complete a transaction without the assistance of Alice. However, Alice may need to assist in making decisions and taking actions to modify the Pass, Event, etc. (to Bob's requirements) in some manner and needs to authorized for selling a modified version of the Pass.
    - Note: discussion of whether Alice is a true "VC Issuer" of an Attraction Pass in this scenario is beyond the scope of this document.

Take 1 Verifying Certificates, Trust Relationships w Issuers, Authorities via a GLEIF approach

GLEIF's approach provides technologies that provide cryptographicly verifiable authority chains such that you can do the following type of on-demand run time verification.



Steps:

1. Bob connects to the A1 Digital Sales Agent and requests certificate validation of
    a. The Sales Digital Agent as a valid services of A1
    b. Alice's Role as Sales Agent for A1
    c. A1 as a valid legal entity
    d. A1 as an accredited Attraction Seller
2. Bob is provided with the DIDs of and access to the certificates of the Sales Digital Agent and Alice.

3. Bob invokes an API to cryptographically verify the path through Alice's certificate to A1, from A1 to the Object Identification Issuer (and that the OEIO is valid for this Jurisdiction) and from A1 to the Attaction Ecosystem Authority
4. Same as 3, but for the Sales Digital Assistant

Pause - *how does this work for organizations not employing GLEIF tech?*

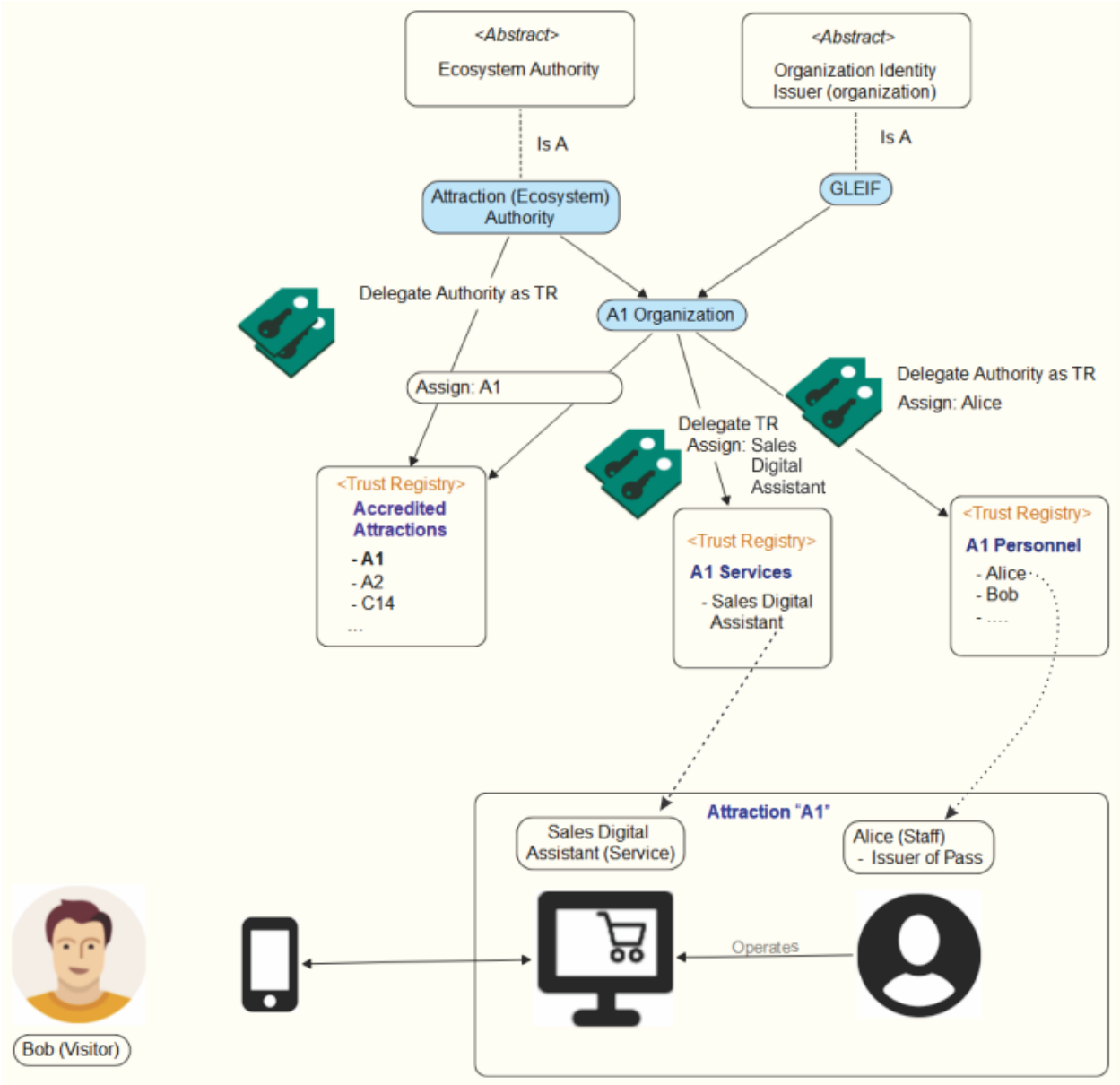
As has been discussed, the GLEIF approach is a large commitment to a new approach and new technology.

Reality check is that for existing organizations not actively using VCs or using VCs without the cryptographically verifiable on-demand linkage between certificates, issues and authorities, this is too big a leap.

The current reality is that most organizations have governance and relationships between authorities, issuers, certificates, etc. which is not fully integrated and on-demand run-time capable.

A much more attainable approach may be through Trust Registries, which many organizations may be already using (e.g., lists of trustable organizations, services, etc.) or which are not a large change (e.g., merging w DNS' infrastructure, particularly DNSSEC.

Take 2, Verifying Certificates, Trust Relationships w Issuers, Authorities via Trust Registries

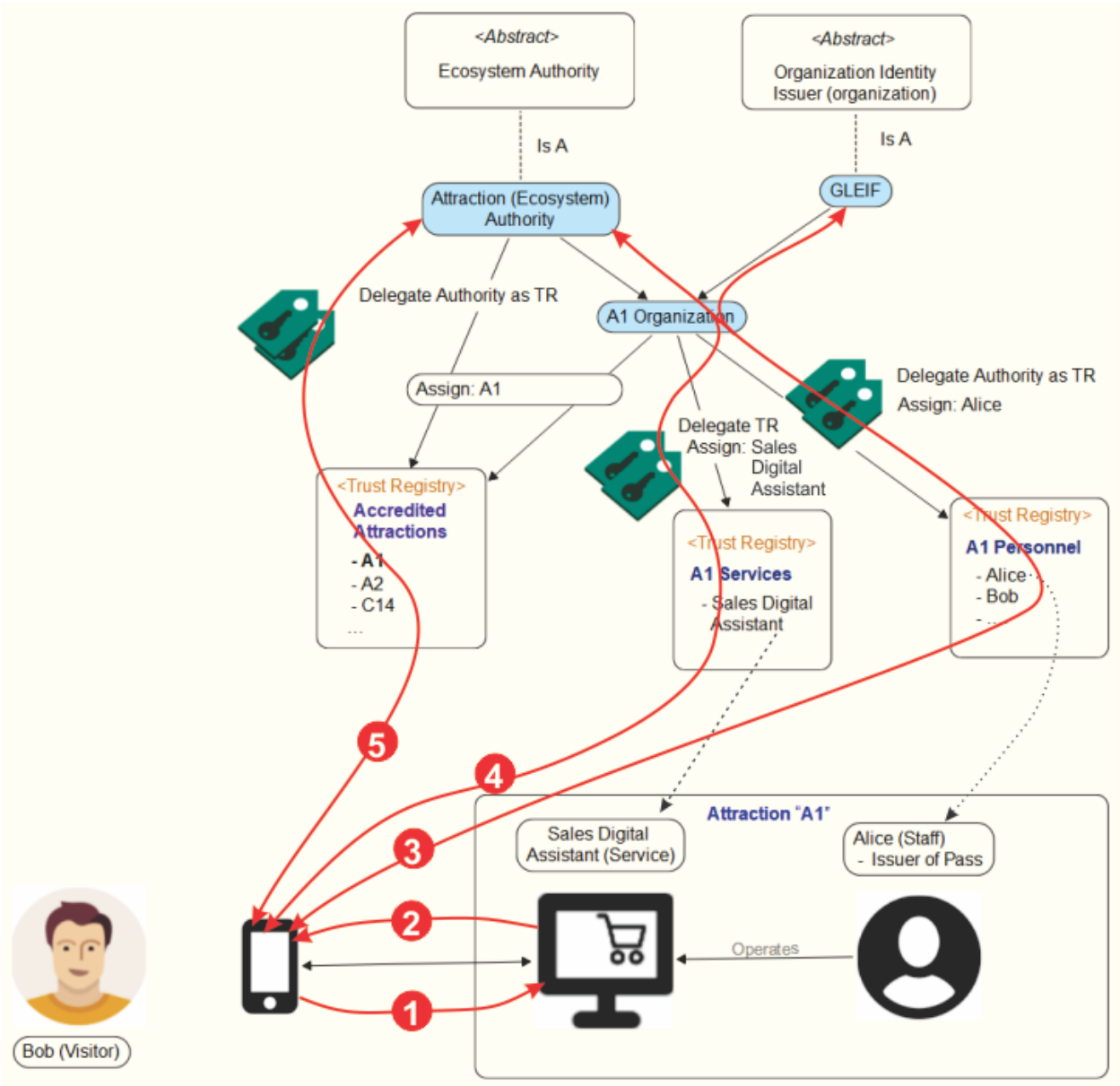


Assumptions for the above diagam (which needs some work)

- The same certificates are issued as per Take 1 and server for primary validation
- Issuers have certificates (issued by a higher authority), but are trusted (not shown) by being entries Trust Registries
    - A VC (from Issue Q2) will list the DID of the Issuer and it's end point (other ways to do this, but let's go for this for now)
    - The DID Document of the Issuer will contain a list of Trust Registries containing the Issuer (likely including a primary TR), which a Verifier can separately validate that the TR selected belong to an Ecosystem Trust List

        - Assumption: an ecosystem will maintain a top level set of Trust Registies for which a graph of Trust Registries exist which can be search by DID (or similar)
- The Attraction Ecosystem will maintain a TR of Accredited Attractions, to which A1 will be admitted, only if it has a Oragnization Identity Issued LEI (or equivalent) and meets the Attraction Ecosystem requirements
    - In the TR, A1 has an entry that points directly or indirectly to it's Trust Registries of A1 Services and A1 Personnel

This set of relationships allows a variation of Take 1's workflow to verify the certificates and relationships via publicly visible Trust Registries



Steps:

1. Bob connects to the A1 Digital Sales Agent and requests certificate validation of
    a. The Sales Digital Agent as a valid services of A1
    b. Alice's Role as Sales Agent for A1
    c. A1 as a valid legal entity
    d. A1 as an accredited Attraction Seller
2. Bob is provided with the DIDs of and access to the certificates of the Sales Digital Agent and Alice, plus certificate of the A1 Organizatin
3. Bob requests the DID of the Issuer for Alice's certificate
    a. Uses the Issuer DID document to locate the A1 Personal TR
4. Bob requests the DID of the Issuer for the Sales Digital Assistant certificate
    a. Uses the Issuer DID document to locate the A1 Services TR
5. Bob requress the DID of the Issuer for the A1 Organization as an Accredited Attraction (Seller) Organization
    a. Uses the Issuer DID document to locat the Accredited Attractions TR
    b. From the A1 entry, which has the A1 Services and A1 Personel registry as properties (or indirect properties), which completes linking the certificates.

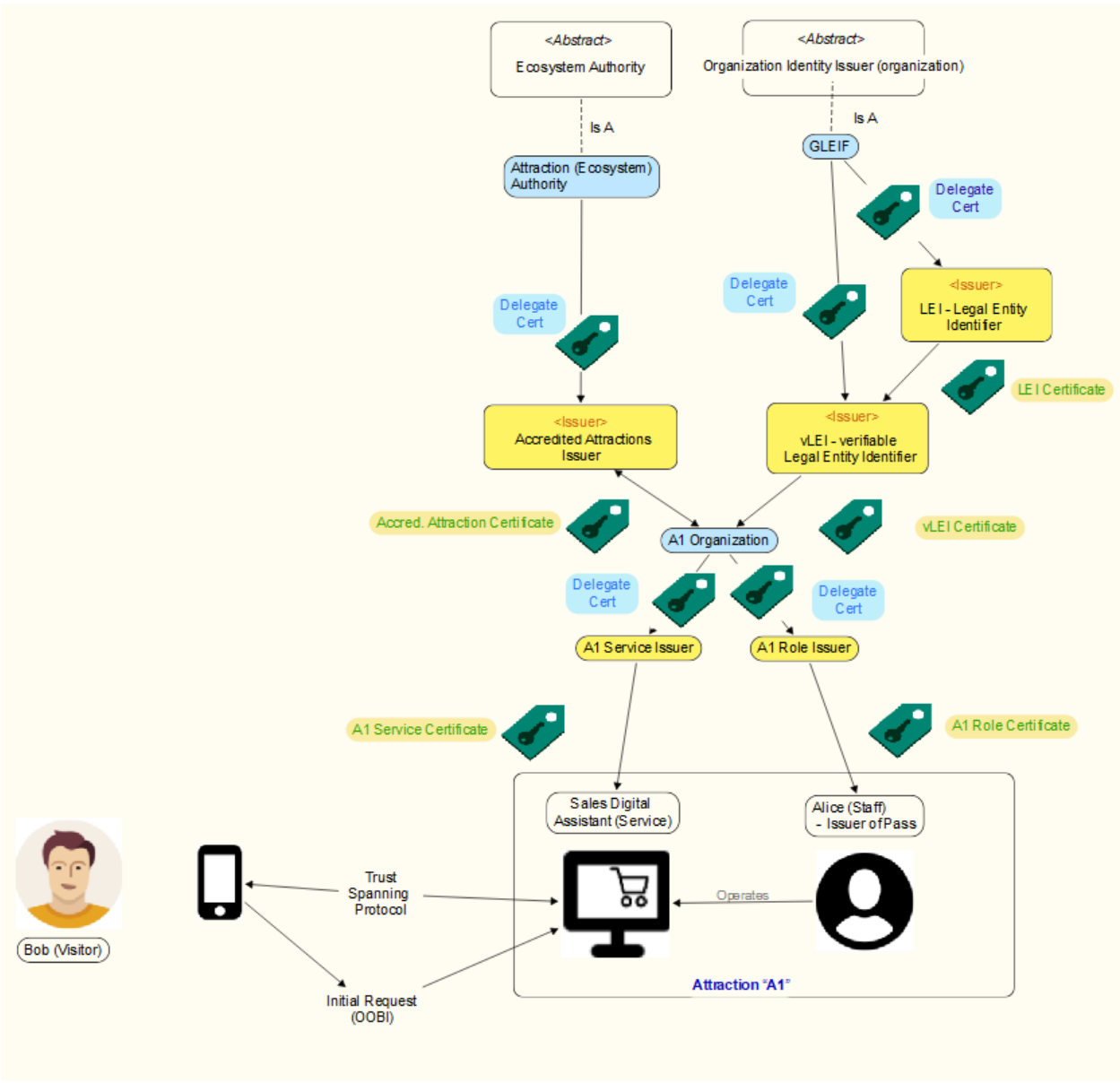
The above sequence is very "draft", but points out that rather than following cryptographic (Sam's ACDC) chains, it is following a series of endpoints and straight forward graph search functions via Trust registries, with a fairly straight foward mechanism to link Credentials, Issuers and Trust registries containing Credentials

Appendix

More complete Certitificate View

The following view is more complete in showing all the certificates and how they are granted.

Note that there are delegation certificates for Issuers in that an Authority such as the Attraction Authority can delegate to Authority to an Issuer to Issue credentials (in this case Accreditation of an Attraction VC) on it's behalf.


<Abstract>
Ecosystem Authority
<Abstract>
Organization Identity Issuer (organization)
Is A
Is A
Attraction (Ecosystem) Authority
GLEIF
Delegate Cert
Delegate Cert
Delegate Cert
<Issuer>
LEI - Legal Entity Identifier
LEI Certificate
<Issuer>
Accredited Attractions Issuer
<Issuer>
vLEI - verifiable Legal Entity Identifier
Accred. Attraction Certificate
A1 Organization
vLEI Certificate
Delegate Cert
Delegate Cert
A1 Service Issuer
A1 Role Issuer
A1 Service Certificate
A1 Role Certificate
Sales Digital Assistant (Service)
Alice (Staff) - Issuer ofPass
Operates
Trust Spanning Protocol
Initial Request (OOBI)
Bob (Visitor)
Attraction "A1"