What does it do?

- Discover credentials and capabilities associated with a well known digital resource.
- Help brands establish trust in related digital credentials.
- logistics.example
  - GET https://logistics.example/.well-known/keys
  - issuers/holders/verifiers.txt
  - dig server.ns.example. _tbd_.logistics.example. TLSA
  - Which signature algorithms are supported?
  - Which types of credentials are issued or verified?
  - Which issuers are supported?
What does it do?

- **Identifier**: SPICE Discovery
- **Verification Keys**
- **Capabilities**
- **Credentials**
- **2001:DB8:0:0:8:800:200C:417A**
- **vendor.example**
- **urn:uuid:19db223b-1b57-4610-b27d-fef6ae8883a4**
- **https://vendor.example**
- **bar codes, qr codes, nfc, rfid, etc... ?**
Why do it?

- Improve assurance by relating confirmation methods to resources
- Help search engines and bots find and authenticate digital product passports and legal entity credentials
- Support new signature algorithms or more privacy preserving credential types as they become available
- Integration point for discussing digital credentials with other IETF stakeholders including SCITT, OAUTH, DIEM, etc.
Status

- Published -00:
  - Need to clarify scope
    - URIs only? URNs?
    - DNS, HTTPS, MOQ?
  - Support DIEM use cases?
  - Relationship to related work?
    - Decentralized Identifier Resolvers
    - OpenID Federation
Next Steps

- Not ready for adoption

- Which protocols and transports need SPICE discovery?

- Perhaps better to spend some time with use cases first?