Applicant/Subscriber

• Every certificate must have an applicant (even if not named in the certificate) \(^{(BR \, \text{§4.1.2)}}\)

• Applicant and Subscriber are the same entity: “Applicant: The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber” \(^{(BR \, \text{§1.6.1 “Applicant”)}}\)

• Responsible for the private key: “Applicant to take all reasonable measures to maintain sole control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate” \(^{(BR \, \text{§9.6.3 #2)}}\)

• Responsible for accepting Subscriber Agreement (or Terms of Service)
Subject and Subject Identity Information

• **Subject**: The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber. *(BR §1.6.1)*

• **Subject Identity Information**: Information that identifies the Certificate Subject. Subject Identity Information does not include a domain name listed in the subjectAltName extension or the Subject commonName field. *ibid.*

• Subject Identity Information is optional – certificate might not have any

• Guidelines call out some specific attribute types for Subject Name:
  organizationName, streetAddress, localityName, stateOrProvinceName, postalCode, countryName, organizationalUnitName, businessCategory, EV jurisdiction, serialNumber, givenName, and surname
Subject/Applicant Relationship

“The Subject is either the Subscriber *(Applicant)* or a device under the control and operation of the Subscriber *(Applicant).*” *(BR §1.6.1 “Subject”)*

“If the Subject Identity Information is to include the name or address of an organization, the CA SHALL verify the identity and address of the organization and that the address is the Applicant’s address of existence or operation.” *(BR §3.2.2.1)*

“If the Subject Identity Information is to include a DBA or tradename, the CA SHALL verify the Applicant’s right to use the DBA/tradename” *(BR §3.2.2.2)*

“the CA implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject” *(BR §9.6.1 #2)*
Subject Alternative Names

- Fully Qualified Domain Names, Wildcard Domain Names, .onion names, and IP Addresses
- Applicant relationship options:
  - Applicant is the Domain Name Registrant \((BR \S 3.2.2.4 \#1)\)
  - Applicant demonstrates authority to request a Certificate for the specific Domain Namespace \((BR \S 3.2.2.4 \#5 \& \S 1.6.1 \text{ "Domain Authorization Document"})\)
  - Applicant demonstrates “control” via one of the enumerated processes \((BR \S 3.2.2.4)\)
Possible Discussion Items

• Should Subject Identity Information be required to identify the Subscriber?

• Should the Subscriber be required to have “sole control” of the private key?

• Should the Subscriber have an obligation "to install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate”? What is the definition of accessible? (BR §9.6.3 #4)

• What relationship, if any, is required between the identified subject and the domain name registrant(s)?