FBCA Supplementary Antecedent, In-Person Definition

This supplement provides clarification on the trust relationship between the Trusted Agent and the applicant, which is based on an in-person antecedent identity proofing event. An Antecedent event is an in-person proofing event that occurred previously and may suffice as meeting the in-person identity proofing requirements. The FPKI Policy Authority (PA) has determined the need for policy specification on methods of performing identity proofing and clarification for use of an antecedent in-person identity proofing process.

The Federal Bridge Certification Authority (FBCA) Certificate Policy (CP) reference to antecedent is *3.2.3.1 Authentication of Human Subscribers* for Medium Assurance (All policies). The requirement for antecedent is identical with the exception of using a historical in-person ID proofing event. Hence, a proposed antecedent process must 1) meet the thoroughness (rigor) of the in-person event, 2) provide supporting ID proofing artifacts or substantiate the applicant through a relationship, and 3) bind the individual to asserted identity.

Two generic use cases have been identified as valid antecedent processes:

1. Sponsor Antecedent, where the applicant, such as an employee, member or associate has no reasonable access to the Registration Authority (RA). The Sponsor will attest to the validity of the individual through their on-going relationship, date of antecedent event and provide unique applicant identity information to RA. Applicant will be bound remotely with known attributes or shared-secrets.

2. Third-party Antecedent, where identity proofing is performed by multiple parties, Sponsor, Entity PKI and trusted third-party or Identity Verification Provider (IVP). In this model, the Identity Verification Provider collects the in-person proofing antecedent artifacts. Sponsor will attest to the validity of the individual through their on-going relationship and provide unique applicant identity information to RA. Applicant will be bound remotely with known attributes or shared-secrets. The date and supporting artifacts verifying the historical identity proofing event are provided to the RA. Trusted parties are required to have a contractual relationship with at least one other trusted party.

An Antecedent process requires various actors, roles, responsibilities and activities. These sections outline specific requirements for the process.

1. ID Proofing Relationships

- The entity performing the identity proofing, Identity Verification Provider or Sponsor of the applicant shall have a contractual relationship with the Entity PKI.

- Sponsor or Identity Verification Provider shall have an established relationship with applicant. The relationship must be sufficient enough to enable the authenticating entity to, with a high degree of certainty, verify that the person seeking PKI certificate is the same person that was identity proofed.

- Sponsor's application shall contain a description of the relationship with applicant describing the initial identity proofing or qualifications and the on-going relationship.

2. Antecedent in-person identity proofing event

- Applicant to provide Federal Government-issued Picture I.D., or two Non-Federal Government I.D.s, one of which shall be a photo I.D. (e.g., Drivers License).

- Trusted Agent or an entity certified by a State or Federal Entity as being authorized to confirm identities is required to obtain applicant's signature. The entity confirming the identity's signature or auditable confirmation of identity proofing process is to be recorded.

3. Entity PKI
   - The Entity PKI shall record the date of the antecedent in-person identity proofing event.

   - The Entity PKI shall obtain any historical artifacts from the Antecedent event.

   - The date of the antecedent identity proofing event shall be the basis for determining the timeframe for the next identity registration event required by Section 3.3.1 of the FBCA CP.

4. Information source requirements.

- The Antecedent process shall use information acquired from an Identity Verification Provider to identify an applicant. When information is obtained through one or more information sources, an auditable, chain of custody shall be in place.

- The Antecedent process shall require that all data received from Identity Verification Provider (including the Antecedent) shall be validated, protected, and securely exchanged.

- All participants shall store and exchange private information in a confidential and tamper evident manner, and protect from unauthorized access.

5. Binding the certificate request to the identity.

The process to bind the claimed identity to the specific certificate request shall provide commensurate levels of assurance with the certificate being issued.

- A Sponsor for the applicant shall provide the Entity PKI with initial contact information, (e.g., name, email address, phone number, sponsoring organization).

- The PKI shall use the sponsor provided information to contact the applicant.

- Applicant, using a prescribed method, shall initiate the credentialing process by identifying themselves through a series of initial questions. At least one question shall be derived from private information occurring in the course of the in-person Antecedent event. This identity binding process shall not be repeated in the event of failure.

- If successful, applicant proceeds to a second phase of questions. This on-line verification process shall be a set of additional (non-repetitive) questions. The system shall score the responses and determine the probability that the claim is or is not fraudulent.

- The identity score is provided to the Entity PKI, and shall be evaluated at the associated level of risk for the certificate assurance level prior to its issuance.

Entity PKI's application shall contain a description of their on-line verification methodology.

6. On-Line Verification Methodology

The On-Line Verification Methodology provides the basis for binding the identity asserted by the remote applicant and verifying the applicant's identity claim. The Identity Verification Provider generates a challenge/response question and answer (Q&A) process, and requires the applicant to successfully reply to the provided questions and offered answers. The Identity Verification Provider shall construct the Q&A process from multiple historical antecedent databases. The Q&A will have a time limit for applicant response. The methodology will support a secondary phase for unsuccessful initial attempts. Results are reported to the Registration Authority.

When selected for on-line verification, the applicant shall be provided with a set of questions. The presented questions shall have these or greater characteristics:

1. Be drawn from multiple and appropriately secured, data sources
2. Five (5) or more questions, drawn from the applicant's identity and historical events records with a minimum of five (5) possible answer choices per question
3. Be administered immediately following or sequentially from the successful identity binding with the Registration Authority (RA), described in Section 5 above.
4. Apply a two (2) minute time constraint to the duration for completing the question and answer activity
5. Require 4 out of 5 correct answers (80%), as a minimum response
6. Offer one (1) additional re-take in the event of a failed attempt
7. During the re-take, replace a minimum of forty (40%) per cent of the prior questions
8. Report the question and answer results to the RA for determination of certificate issuance

The methodology provides a baseline for an acceptable process standard for auditability and implementing other qualified processes.

GLOSSARY

Certification Authority (CA)	An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CARLs or CRLs.
Certification Authority Revocation List (CARL)	A signed, time-stamped list of serial numbers of CA public key certificates, including cross-certificates, that have been revoked.
Certificate Policy (CP)	A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.
Certificate Revocation List (CRL)	A list maintained by a Certification Authority of the certificates which it has issued that are revoked prior to their stated expiration date.
Entity PKI	For the purposes of this document, "Entity" refers to an organization, corporation, community of interest, e.g. association, or government agency with operational control of a CA.
FBCA	Federal Bridge Certification Authority
Identity Verification Provider	An organization providing individual, identity information and databases used for identity verification. This information shall be available records of historical identity and

	authentication transactions. These historical database records shall include appropriate identity and authentication (I&A) attributes meeting FBCA CP requirements. The databases include referenced original source data and where copies of the data are utilized, integrity and chain-of-custody of the data must be auditable. These organizations must be able to demonstrate through Policy and Audit that the data is accurate and maintained with appropriate integrity, privacy and confidentiality.
Registration Authority (RA)	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA).
Sponsor	An organization participating in or a member of a community of interest and/or association operating an entity PKI that provides a common policy, guidelines and rule set requiring consistent implementation and operations. This Sponsor shall maintain a continuous relationship with applicant through certificate life cycle.