# Assumptions and Notes about InCommon Silver Compliance

## Assumptions and Notes about InCommon Silver Compliance

*Please insert sub-bullets for any assumptions or other observations about your campus's InCommon Silver compliance that you feel would be of interest to other campuses.*

- UCB
- UCD
- UCI
- UCLA
- UCM
- UCR
- UCSD
    - **Credential Issuance (4.2.4.1)**
        - "…the Subject shall identify himself or herself in any new transaction (beyond the first transaction or encounter) with information known only to the Subject…"
            - My concern is just how secret does the secret have to be to assume that only the Subject knows it? They mention a temporary secret as an example, either established during a prior transaction or sent to the address of record, but clearly e-mail administrators could learn the secret when sent via email or the registration agent might be able to see the temporary secret during registration. Is it even possible to meet this requirement as stated? It seems that at the very least, a system administrator could read the secret from memory as it is established.
- UCSF
- UCSB
    - **Approach and Assumptions**
        - We are defaulting all local identity to so-called Bronze level. Silver level requires an uplift process for those demographics that are eligible for silver.
        - We are not questioning or evaluating any externalities such as PPS or student registration. From a business perspective, they are completely separated from IdM and we are logically required to assume that other units within the university follow their published policies and practices. In part, this is our finesse of certain questions. For example, we don't question common name (cn). Since we populate it from its data of record, we follow the practices of the processes that create the data of record, in this example PPS for employees.
        - We are going with the one id and two passwords design. They will be in physically separate repositories.
        - We currently require employees to present themselves in person at the Identity desk even after an I-9 verification. We are hopeful that in the forthcoming PPS/HRIS replacement project we will be able to tie it to the creation of identity within the IdM, and thus eliminate the second in person verification of credentials.
        - We could not come up with a combination of KBA characteristics, the query of which we believe satisfies identification. A number of us know how to acquire ssn, dob, etc. for any person, and are thus uncomfortable with other than a genuine shared secret known only to the principal and the provisioning system.
        - Our design incorporates the notion of LOA-0 principals (our definition) who we will never federate even though they are present in the directory. We are using this for a class of principals who self-register with no supporting IVP whatsoever.
- UCSC
    - **General Questions**
        - Is there an assumption that when we assert a givenName/sn for a Subject with a Silver IAQ that the name we provide is the name on record? (E.g., "legal name" and not "name I like to be called")?
    - **Define:** Registration
        - I assume that "IdPO Registration" refers to the process of creating a new identity/person record in whatever system is the source of that record. So for UCSC, the Registration is the entry of a student record into the student system, of an employee record into (one of) the HR system(s) or of a "sundry" record into the IdMS itself.
    - **General IVP Questions**
        - In many cases we generate and distribute credentials "in advance", without much identity vetting, and then later do an identity vetting of the individual. E.g., we create an account for a Subject with an informal employment offer (who is not in PPS), provide the (presumed) Subject with the credential, and then later do an in-person or remote verification of the Subject (I-9 verification, entry into PPS).
          In these cases it's difficult to assert that the person we originally distributed the credential to is the same physical Subject as goes through the IVP, since there was no real IVP (at least not beyond Bronze level) of the initial, non-validated credential distribution. What's an appropriate level of "retroactive verification" of the account delivery in these cases?
    - **Registration and Identity Proofing (4.2.2.3)**
        - This language is in the section on "Registration" but it seems to be describing how to do Identity Proofing for Credential Issuance (the language in Credential Issuance says "Identity Vetting must meet same strength as in 4.2.2.3"). It's unclear to me what is required for verifying an "Address of Record" when the Registration Record is being created. Is this intended to be equivalent to a credit-check or some other 3rd party address verification process?
    - **RA Authentication (4.2.2.4)**
        - Assuming this refers to the credentials used to log into the systems where Subject records are created. E.g., PPS.
- LBNL
- UCOP