# Traversing the Web of Trust:
# A Protocol for Trusting the Issuer of a Verifiable Credential

Stephen Curran, Cloud Compass Computing, Inc.
Contractor to the Government of British Columbia

The successful verification of a Holder's Proof built from a Verifiable Credential provides the verifying party with some useful technical information:

- That the party delivering the claim is it's Holder
- The identity (Decentralized ID or DID) of the Issuer of the Credential
- The credential data has not been tampered with since its issuance
- The Credential has not been revoked by the Issuer (proof of non-revocation)

What the Verifier does not know without some further effort is: should they trust the Issuer of the credential? In the offline world, the trustworthiness of a credential from an Issuer is usually a person recognizing the validity of a document that the holder provides - a passport, a driver's license, a document from a known utility company, and so on. Depending on the purpose of the verification, the choice of documents and level of scrutiny applied varies from, for example, scanning a letter from a utility company for its logo and the data of interest to verify a place of residence, to the rigorous visual and technical inspection of a passport before crossing a border. It is not obvious how to achieve that same level of trust in an automated, scalable online transaction.

This note proposes the use of "Accrediting Authorities" and a related Verifiable Credentials-based protocol for implementing a scalable, automated mechanism for determining the trustworthiness of an Issuer, including support for an offline component when the automated process does not produce a result. In this context, "Accrediting Authorities" are oversight or affiliation organizations consisting of entities "registered" via some type of verification process to be included as members. For example, professional organizations, trade associations, regulatory groups and various government services all might be Accrediting Authorities issuing Verifiable Credentials about entities registered with those organizations. The degree of trust an entity gains through their membership in a Accrediting Authority is proportional to the level of effort required to register with the Accrediting Authority - something that must be assessed by a person based on the purpose of the claims they are verifying. For example, a Professional

Association that requires specific, Verified Credentials to join is likely more trusted than one requiring only a small payment to join.

The protocol outlined here supports a consistent, automated technical process for navigating from the DID of the Issuer through a chain of Accrediting Authorities to establish the trustworthiness of that Issuer. Further, the protocol supports the collection of information to initiate a human review of the trustworthiness of the Issuer, enabling bootstrapping trust through the creation of Lists of “trusted” and “not trusted” Accrediting Authorities.

## Initial State: No Trusted Issuers

The Verifier initially starts by verifying a Proof created from one or more Verifiable Credentials received from a Holder and issued by an Issuer(s). As noted above - the Verifier knows some technical facts about Proof from a successful verification, including the DID of the Issuer, but they do not know how to decide whether or not to trust the Issuer. If they could, they could also decide whether or not to trust the claims offered by the Holder/Prover.

By resolving the DID, the Verifier can access the related DID Document and request a Proof of a Verifiable Credential from the Issuer that can contribute to whether the Issuer can be trusted or not. To automate the process, a standardized information structure from an organization to attest to the trustworthiness of the Issuer is proposed. The process is recursive - can the organization attesting to the trustworthiness of the Issuer itself be trusted?

## Accrediting Authorities and Accrediting Authority Verifiable Credentials:

Accrediting Authorities are existing (“real world”) organizations that issue Verifiable Credentials about entities that in turn issue Verifiable Credentials.  The precise content of the Verifiable Credential issued by the Accrediting Authorities could be formalized, perhaps based on specifications such as the Electronic Signatures and Infrastructures (ESI) Trusted Lists[1] that is used by the EU. Without going deep into such a specification, assume the Verifiable Credential would include at least the following information:

- Entity Name - the legal name of the member entity
- Entity ID - the ID of the entity within the Affiliate Organization
- Entity URL - the URL published by the member entity
- Affiliate Organization Name - the name of the organization of which the entity is a member
- Entity Member Type - the Type of member of the Accrediting Authority Owner Organization

[1] http://www.etsi.org/deliver/etsi_ts/119600_119699/119612/02.02.01_60/ts_119612v020201p.pdf

- Entity Type Policy URL - a URL containing a description of the process used to achieve a type of affiliate membership
- Member Since Date - the Date the member entity joined the organization
    - The definition of that Date should be defined in the Entity Type Policy
- Membership Expiration Date - the expiration Date of the member entities current membership

## The Online Process:

The online process is performed for each of the Issuers identified by the Verifier as having contributed to a Proof. In the following there is a simplifying assumption that each entity is a member of just a single Affiliation (Accrediting Authority). However, that need not be the case and where there are multiple Affiliations, the process expands to traverse each trust path as necessary.

The following defines the full sequence of the automated process to determine if an Issuer is “Trusted”, “Not Trusted” or if additional offline evaluation is required. Note that this is a recursive algorithm, and the Issuer changes for each recursive call. Where necessary, the term “original Issuer” is used to reference the Issuer of the Verifiable Credential that initially triggered the process.

The description of the related offline process is defined in the next section.

- The Verifier checks the Issuer DID and stops the process if the Issuer is known to be Trusted or Not Trusted. If neither, the process continues.
    - If the Issuer is not the Original Issuer, the result will include if the “Trusted” / “Not Trusted” results apply to the Issuers ancestors.
    - The “Trusted or Not” status stored by the Verifier is essentially a cache of previous traversal results. The handling of this “trust cache” would be managed by the Verifier based on the frequency of use and risk associated with the verification.
- The Verifier resolves the Issuer DID to retrieve the associated DID Document of the Issuer of the Credential.
- The Verifier constructs a Proof Request to the Issuer for a Proof of a Accrediting Authority Verifiable Credential. If the Issuer is unable to satisfy the Proof, the process stops with a status of “Unknown”.
- If the trustworthiness of Accrediting Authority members of the Type of the Issuer is known, the Issuer is marked as “Trusted” or “Not Trusted”, the process stops, and the result is returned.
    - Otherwise, the Verifier retains the information from the Proof and the process continues.
- The Verifier makes a recursive invocation of the process, this time with the Issuer being the Issuer of the Accrediting Authority Verifiable Credential.

The recursion repeats until a “Trusted”/”Not Trusted” status is found for an Issuer or an Issuer is found with no Accrediting Authority Verifiable Credential, meaning the result is “Unknown”.

At the completion of the online process, the original Issuer will have a status of Trusted, Not Trusted or Unknown. If the status is Unknown, the information derived from executing the Online Process is consolidated and queued to trigger the execution of an offline process.

## Offline Process

If the Issuer is unknown to the Verifier via the online process (e.g. a “Trusted”/”Not Trusted” decision was not made), the request to vet the Issuer and its Accrediting Authority hierarchy is queued up for a person to complete. The request includes all the information collected about the Issuer and its Accrediting Authority hierarchy (if any).

- If only the DID of the Issuer is known, use the DID Document contents to investigate the Issuer, much as one would investigate an organization given it’s public Web URL. As needed, online and offline contact may be needed with the organization, or to others that might know of the organization. At the completion of the investigation, the Issuer would be designated as “Trusted” or “Not Trusted”.
  - The designation is used as the result of the current request, and recorded in a list for future executions of the process.
- If a populated Accrediting Authority hierarchy (of one or more links) of affiliations is found, an investigation of the information and web links from the Accrediting Authority proofs about the affiliates would be conducted and for each, a “Trusted” / “Not Trusted” decision made. Further, the scope of each decision would also be recorded - does it include just the affiliation organization, or does it also include all members of the given type of the organization?

At the conclusion of the Offline Process, one or more “Trusted” / “Not Trusted” decisions would be recorded, including for Accrediting Authorities whether/how the status applies to ancestor entities. With that, the trustworthiness of the original Issuer is known and the process for the Holding entity can proceed.

## Trusted and Not Trusted Lists

If no recording of “Trusted” / “Not Trusted” is made for future executions, the completion of the online process will always trigger an offline process. The online process use the lists as essentially caches of the offline results to automatically complete the process without initiating an additional offline investigation. Policies around length of time to cache the list entries would be established by the Verifier organization, and would probably (for a “Trusted” list at least) be driven off the “Membership Expiration Date”. Policy-driven periodic online processes could be executed automatically (independent of Holders) to maintain “Trusted” / “Not Trusted” lists - e.g. to update the status of affiliate organizations.

Note that the offline process is focused on the trustworthiness of the ***Issuer and its Affiliation hierarchy*** - not on the Subject of the process currently in progress (the Holder), since the Proof delivered by the Holder was successfully verified. For example, if the process is to vet the Academic Credentials of a Job Candidate, the Proof has already confirmed the provided Credentials are valid - but not that they were issued by an accredited institution.

The scope of the result of the offline investigation might be just the Issuer, but it might (ideally) include all Issuers that are part of a given Accrediting Authority - for example, members of an organization of accredited institutions.

## Shared Trusted/Not Trusted Lists

The process described above requires the bootstrapping of the Trust Hierarchy from no information for each Verifier. This implies that some effort will be required to perform offline research to build up the Trusted / Not Trusted lists. Given this consistent structure, it’s likely that organizations might share their Trusted / Not Trusted list, and there might be a financial incentive for an organization to build and share curated lists. Such sharing could reduce the manual effort by each organization to bootstrap their Issuer Trust data.

## Online-Only Accrediting Authorities?

While in theory the processes outlined here may trigger the creation of Accrediting Authority entities solely for the purpose of supporting this protocol, in practice, that should not occur in the common case since the goal of this protocol is to establish online trust based on “real world” trust. Accrediting Authority operators exist for “real world” purposes and their online Accrediting Authority role is a side-effect of that real world role. Thus, it’s likely new Accrediting Authority-type organizations would come into existence only for “real world” purposes - not to just enable online Trust. In fact, an online-only Accrediting Authority might be a red flag in establishing trustworthiness.

# Appendix A: Trust Traversal Example

Here is an example of this process working for the Alice/Faber/Acme transcript example. The following is divided into 3 sections:

- Before the proof is delivered to Acme
- During the delivery/evaluation of the Alice proof
- During the delivery/evaluation of the Bob proof - a second, similar proof.

The interactions are listed at a high level and assume that the underlying details are understood. Some notes:

- The shorthand VC(name) and Proof(name) are used to indicate a Verifiable Credential or Proof is used about the topic “name”.
- “th” is used as a shorthand for a Accrediting Authority VC or Proof.
- The shorthand “A→X→B” means that A delivers X to B
- The “Before” and “During” processes are the first time through processes - e.g. when the network and all the participants are using the network for the first time.
- Only the “Trusted” list is referenced, but of course there would be a corresponding “Not Trusted” list as well, and a process result of “Not Trusted”.

***Aside**: In this process an entity might be a member of multiple Accrediting Authorities and it would be useful for the Verifier to know about all of them. As  such, this is a use case (and there are others I have encountered) where it might be nice to have a method of getting multiple Proofs returned from a single Proof Request. A separate, but interesting issue from the focus of this note.*

## Before:

- US Gov (USG) is a Accrediting Authority for US Government entities, including the Dept. of Education (DoE)
    - USG → VC(th) → Dept of Education (DoE)
- DoE is a Accrediting Authority for organizations of educational entities
- Accredited Colleges & Universities (AC&U) is a Accrediting Authority that is recognized by DoE
    - DoE → VC(th) → AC&U
- Faber College is accepted into AC&U
    - AC&U → VC(th) → Faber
- Dickinson College is accepted into AC&U
    - AC&U → VC(th) → Dickinson
- Faber → VC(transcripts) → Alice

- Dickinson → VC(transcripts) → Bob

## During Alice Proof Process:

- Acme → ProofReq(transcripts) → Alice → Proof(transcripts) → Acme
    - Acme extracts Faber DID from Proof
        - DID on Trusted List?  No - continue
- Acme →ProofReq(th)→ Faber  → Proof(th) → Acme
    - Acme extracts AC&U DID from Proof
        - DID on Trusted list? No - Continue
- Acme →ProofReq(th)→ AC&U →Proof(th)→ Acme
    - Acme extracts DoE DID from Proof
        - DID on Trusted list? No - Continue
- Acme →ProofReq(th)→ DoE →Proof(th)→ Acme
    - Acme extracts USG DID
        - DID on Trusted list? No - Continue
- Acme  →ProofReq(th)→ USG
    - USG has no proof to send to Acme
        - Trigger Offline Process
- Acme personnel research the chain of information available from Accrediting Authoritys and decides to:
    - Add USG, DoE, AC&U and Faber DIDs to the “Trusted” list
    - Trust the transcripts Alice provided because they come from Faber
- Traversal Result: **Trusted**

## During Bob Proof Process:

- Acme → ProofReq(transcripts) → Bob → Proof(transcripts) → Acme
    - Acme extracts Dickinson DID from Proof
    - DID on Trusted List?  No - continue
- Acme →ProofReq(th)→ Dickinson → Proof(th) → Acme
    - Acme extracts AC&U DID from Proof
    - DID on Trusted list? Yes
- Process Result: **Trusted**