How To Constrain Multichannel Vetters

1. Vetters receive a "Vetter Certification" credential. This credential has the following fields that impose constraints on the vetter:

   ECC Targets: list of e164 country codes in which the target of this vetter's attention may possess a phone number for which the vetter is certified to attest right to use.

   Jurisdiction Targets: list of ISO 3166-1 country codes for this vetter is certified to attest incorporation, legal correctness, and legal entitlement to use brand assets.

2. Suppose Certification_A (vetter A's certification credential) has this content:

   ECC Targets: ["44", "91", "33", "1", "34", "81", "66", "971"]
   Jurisdiction Targets: ["GBR", "ZAF", "THA", "BRA", "USA", "FRA"]

   And Certification_B has this content:

   ECC Targets: ["33", "91", "81", "66", "27", "971"]
   Jurisdiction Targets: ["FRA", "ZAF", "THA", "IND", "PAK", "USA", "CAN"]

3. Suppose Acme Space Travel is incorporated in France and does business all around the world. Acme wants a dossier that lets them make VVP calls from a UK phone number. They normally do business with Vetter B, so they ask Vetter B to help them. B vets Acme and issues 3 credentials:

   Identity_B: Acme is incorporated in France and has LEI value X.
   Brand_B: According to the laws of France, Acme has the legal right to use the brand name "SpaceMe!" with a cool logo of a rocket ship.
   TN_B: In Vetter B's judgment, Acme has the right to use TN +44xxxxxxxxxx.

   Each of these credentials contains an edge, which is a backlink to Certification_B. (The certification in turn might have a backlink to a vLEI proving GSMA's identity, but that's not relevant here, so I'm ignoring it.)

4. Acme now attempts to create **Dossier_B** (the subscript indicating its dependence on vetter B). Well behaved dossier generation programs will not allow Acme to do this, because it will detect a problem. But let's assume Acme has software that is malicious or badly

written. They put these credentials into a dossier and begin emitting phone calls that reference the dossier. (In a healthy ecosystem, there are multiple enforcement points, but ultimately, any party that has risk can do their own verification, and doesn't trust that someone upstream did things right, so we're going to imagine a situation where that matters.)

5. A verifier gets a phone call from +44xxxxxxxxxx. It is accompanied by a passport that cites $Dossier_B$. The verifier fetches the dossier and in turn, all of the credentials that the dossier references $Identity_B$, $Brand_B$, and TN_B. Because of the backlink in each of these credentials, the verifier also fetches $Certification_B$. It now performs the following analysis (plus some other tests I'm omitting for simplicity):

   - ☑ Is $Dossier_B$ properly signed by Acme and unrevoked?
   - ☑ Are all of the credentials directly referenced by the dossier ($Identity_B$, $Brand_B$, and TN_B plus a delegated signer cred that we're ignoring for simplicity) properly signed and unexpired/unrevoked?
   - ☑ Are all of the credentials indirectly referenced by the dossier ($Certification_B$) properly signed and unexpired/unrevoked?
   - ☑ Are the identity, brand, and TN credentials issued to the same party that signed the dossier?
   - ☑ Does the asserted TN of the call, +44xxxxxxxxxx, correspond to the TN in the TN credential?
   - ☑ Does the asserted brand of the call, "SpaceMe!" with logo, correspond to the brand data in the brand credential?
   - ☑ Does the identity credential say the caller (accountable party) is incorporated in a country that also appears in the Jurisdiction Targets field of $Certification_B$? (Yes, incorporated in France; FRA is in Jurisdiction Targets for Vetter B.)
   - ☐ Does the TN credential say the caller has the right to use a TN whose country code also appears in the ECC Targets field of $Certification_B$? (No, 44 is not in ECC targets for Vetter B.)
   - ☐ Is the caller asserting the brand in a country that also appears in the Jurisdiction Targets field of $Certification_B$? (No, caller is asserting brand in UK, but GBR doesn't appear in Jurisdiction Targets for Vetter B.)

   The answers to the last 2 questions is **No**. *The dossier cites evidence that depends on a verifier who is NOT known to be certified to vet right to use +44 TNs, and who is NOT known to be certified to assert brand right-to-use in the UK.* Therefore, the verification service complains. Specifically, it sets two bits in the evidence status code to communicate that the statuses of the TN credential and brand credential = "does not

apply to this call". The client of the verification API gets to decide whether it considers these bits to be errors (don't route the call), warnings (route but suppress brand), etc.

So let's suppose Acme is unhappy that its calls are being blocked. It realizes the problem and instead approaches Vetter A. It now gets IdentityA, BrandA, and TNA. Acme then builds DossierA and starts sending traffic. Now the verifier repeats the analysis and gets to the last 3 questions again:

- ☑ Does the identity credential say the caller (accountable party) is incorporated in a country that also appears in the Jurisdiction Targets field of Certification$_A$? (Yes, incorporated in France; FRA is in Jurisdiction Targets for Vetter A.)
- ☑ Does the TN credential say the caller has the right to use a TN whose country code also appears in the ECC Targets field of Certification$_B$? (Yes, 44 is in ECC targets for Vetter A.)
- ☑ Is the caller asserting the brand in a country that also appears in the Jurisdiction Targets field of Certification$_B$? (Yes, caller is asserting brand in UK, and GBR appears in Jurisdiction Targets for Vetter A.)

The verification returns an evidence status code indicating that the evidence is solid.

Notes

1. Notice how carefully worded the verification criteria, and the meanings of the constraint fields on the vetter certification credential, are. Saying "Vetter A can vet in the UK" is not precise enough.
2. We could get more granular: Vetter A can make assertions about legal incorporation in jurisdictions X, Y, Z, but can only make assertions about brand licensure in jurisdictions W and Y. (That would require splitting Jurisdiction Targets into 2 fields: Legal Entity Jurisdiction Targets, and Brand Licensure Jurisdiction Targets.) We could also add constraints about the type of company (can vet major corporations but not sole proprietors; can vet in energy and health verticals but not education), call purpose, and dozens of other things.
3. Granularity is a tradeoff. By making vetter certifications granular in this way, we are introducing a lot of expressive power into the ecosystem. However, we are also creating opportunities for confusion, and the need for companies to be vetted multiple times (unless most vetters can operate in most contexts).
4. This shows enforcement at verification, which MUST occur. But could also enforce at signing time (Provenant's signing service will), at dossier creation time, at moment of issuance, etc.