PRACE IOTA Profile response

Change log

Version	Date	Comment	Name
0.1	2013-12-09	First draft	Vincent Ribaillier, Jules Wolfrat
0.2	2013-12-11	Discussed in Security Forum meeting	

* BASIC PREMISES

- Subject names must be globally unique

- Subject names must be persistent (for the life time of the authority)

- It's about people and robots

- Naming of IOTA subjects must be different from other profiles (no overlapping namespaces and no 'migration' between pseudonym and real person with the same full subjectDN)

* REAL NAMES AND PSEUDONYMS

"Do the RPs/RCs need the 'real name' of the person the certificate subject?"

- Is it enough to be able to ask another entity to give you the name (e.g. the VO, community, other site or central LDAP)?

Answer: We don't need the real name in the SubjectDN if we can ask the real name to another entity

What assurance level do you expect from this 3rd party?

Should comply with internal assurance requirements

- Do you need this information up-front (before or at use time)?

Answer: We have the real name now up-front in our LDAP and this will also be required from external entities, at least for some partners/countries

- Do you need this information at end (e.g. for accounting)?

Answer: Not relevant as we already need the real name up-front

or:

- It is sufficient to be able to ask an entity to contact the user on your behalf

Answer: Only if it is possible before an account can be used

(like a privacy forwarding service)?

- Should pseudonyms be clearly identifiable (e.g. if they look like a name they

should be the real name)?

Pseudonyms should be clearly identifiable as such; at least the chance on confusion must be avoided. If names are used or some format which looks like a name this should be the real name.

* COMMUNNITY/VO EXPECTATIONS

"Vetting assurance level and responsibility"

- Given that the name may be a pseudonym and is weakly verified, do you (RP,

or community) have the mechanisms in place to strongly identify the real user?

Answer: in principal we have the mechanism to link the real user to his credential, but we will need stronger verification of the internally used procedures

- Should we enforce obfuscated naming for all subjects?

Answer: Not mandatory

- How will you (RP, VO) deal with ‘identity spoofing’?

Answer: standard incident procedure will be followed, e.g. involve RA of the CA to find out what and how it may have happened.

- How do you currently enrol users in the community? Do you use or rely on the

commonName of the subject for adding people to your databases (or get a

‘warm fuzzy’ feeling in association with e.g. unsigned email)?

Answer: registration in our databases is based on a signed contract with users.

"Traceability by the VO or community"

- Are you set up to provide traceability for your users?

Answer: Not relevant

- Do you have means and procedures for incident response and mitigation?

Answer: Not relevant

* AUDITABILITY AND TRACABILITY FOR RPs AND RESOURCE CENTRES

"Access to the user information by RPs"

- Do you insist that the collection of this data is verifiable?

Answer: Yes

- Should the chain of processes be documented?

Answer: Yes

- Should the chain of processes be audited periodically (expensive!)?

Answer: should be possible in case of doubts

- Should the chain be auditable? Or contract/sanction-based?

Answer: Not relevant. At least we would require a contract or some other statement describing the responsibilities of the chain. We always need the right to end the relation.

- A user may and will have many credentials and changing names: does this pose issues for you?

Answer: No

- Do you expect e.g. the community to provide a real name up-front with every access request (e.g. in a VOMS generic attribute for those using VOMS)?

Answer: Yes

Do you have software able to record that in logs?

Answer: depends on local site procedures, but could be a future requirement

"Do the RPs (RCs) need to be able to independently trace the user without involving the user community?"

- Can a registration mechanism, retrievable or callable by the RP, satisfy this requirement (e.g. like the EGEE CIC portal having an ability to send email to the 'owner' of a DN)?

Answer: In principal we will use our own tracing capability, but an external facility can be used if needed, like information from the CA. So, it's needed as additional facility. CAs can provide this now.

"Can you distinguish between VOs when deciding which user credential to accept?"

Answer: We don't use VOs. Users can work however on different projects and use different credentials.

"Do the RPs need to be able to trace without involving the CA?"

Answer: No.

- Which are the 'emergency cases' where they expect CA involvement in tracing or contacting subscribers?

Answer: In case of suspicion of misuse of a user's credentials.

* INCIDENT RESPONSE

"Do RPs/RCs expect the CA to be involved in incident response?"

Answer: Yes

- What is an incident where you expect CA involvement?

Answer: 1) if used certificates may be compromised, e.g. not properly issued; 2) security leaks in software tools used by CAs; 3) certificates may have been stolen and must be revoked.

- What is the level of involvement?

Answer: as needed. So, this may be all the evidence material that the CA can provide

- Do you see a classification of incidents?

Answer: yes, depending on the impact of the incident.

- If there are up-stream IdPs, are you 'happy' with just the CA response even if upstream IdP does not participate?

Answer: not happy.

- Do you expect more than pure credential revocation in case of demonstrable credential compromise?

Answer: yes, the CA itself may be compromised, so an internal investigation is needed. Or isoftware tools may be compromised

- Do you see the CA more than a fall back to point to in case LEA (Law enforcement Agency) comes after you?

Answer: they must fully cooperate.

- Do you expect/prefer suspension possibilities? Do you have this capability at the RP level (through authorization)?

Answer: we have suspension possibilities and they are mandatory

"Can you get by with just your own response capability?"

Answer: in principal yes, but availability of services may be less than needed. If the CA or IdP doesn't cooperate we have to remove the CA from our trust base, so more users than possibly needed won't have access anymore. So, it's preferred that IGTF and CAs cooperate.