Panel Reports

Panel 1 : « FEDERATED ID MANAGEMENT »

What are the most significant issues?

A/ Legal

- Enforceability
- Transfer of Liability
- Formal
- Dispute resolution
- Constraints/restrictions
- Privacy
- Data protection

B/ Political

- Trust
- Privacy rules
- Control
- Will to share
- Multiple jurisdictions
- National sovereign

C/ Governance

- Policy & rules
- Traceability
- Oversight
- Stakeholders

D/ Social

- Citizen centric
- ID protection
- Impact on people
- Cultural
- Trust
- Control

A/ Significant Legal issues to overcome

1) How to establish the lowest effective common denominator of ID management legislation
    a. NATO policy & legislation will need to look at national legislations but is not bound by any.
    b. All nations do not have clear legislations now
    c. Laws today are all about digital SIG, PKI, etc…

2) The definition of risk and mitigation and appropriate assignment of liability
    a. Governments do not do liability (transparency)
    b. How NATO determines structure for this:
        i. Assessing value of asset (harmonizing)
    c. Provide appropriate guidance of risk assessment/process steps
        i. NATO view of cascading guidance

B/ Significant Political issues to overcome

1) Trust of partners outside of the formal NATO alliance (NGO)
    a. Capability & management of data
    b. Lack of common values for privacy
    c. Rigor in which individuals are vetted
    d. What can be stored and shared between nations
    e. This can be nations or non-nation organizations

2) Impact of changing within NATO nations requirements "after the fact" with participating nations
    a. Significant trust factor
    b. "Unfunded requirements" for infrastructure
    c. Political cost versus Political will

3) Need to be able to "split" the "application" from the underlying "identity"
    a. Explicit willingness to share is impacted
    b. Need globally interoperable EID

C/ Significant Governance issues to overcome
"Executing versus Governance" mediated trust relationship

1) Concern that NATO governance structure may not be able to respond/deploy effectively
    a. "Perception" that nations may have to give up sovereignty
    b. "Least common denominator" not acceptable risk?
    c. Governance may not be effective as an alliance
    d. Community of interest (NATO) may raise "least common denominator"
    e. Needs to be based on risk assessment specific to NATO
    f. May take a "long-long" time and we cannot wait

2) Risk that "bilateral" driven identity federation rules will drop out other NATO participants
    a. "Graded" approach may be necessary
    b. Is it a "trusted relationship" between:
        i. Individual and nation? (root authority –guarantees)
        ii. Individual and NATO?
        iii. NATO Service?
    c. Bi-lateral agreements do not scale –"islands of trust" defeats strength of network

3) Compliance implies that there will be a “super authority”
    a. Networks will become federated:
        i. Will this drive definition of ID Management
        ii. Assumptions need to be revisited
    b. Nations may need to agree: do we want this under Federated or Central management?

D/ Significant Social issues to overcome

1) Increased mobility of persons if we are able to positively validate who people are in AOR:
    a. These are very positive outcomes
    b. “Good for NATO” but what about member nations
    c. Eliminate duplicate and conflicting ID credentials
    d. From NATO perspective – no social issues to overcome

2) When we start “contractualizing” areas/rest, how will NATO manage this?
    a. Effective communications plans
    b. Citizen/participant acceptance of “Big Brother”
    c. If people are “forced” into compliance:
        i. Conscripted forces
        ii. Institutions
    d. Back to “Trust” issue

Panel 2 : « TECHNICAL »

- Definitions
- Review Interoperable (Policy) – Political Net
- Established requirements
- Establish Policy for each area
- Proofing
- Segment Inf. (Classification)
- Establish minimum set of attributes
- Use attributes to address Inf.
- Reference Lab
- Enforcement

Panel 3: « SECURITY »

Started with a briefing to set the scene in terms of Risk Assessment, Accreditation/Evaluation and Evaluation Criteria.

Moved in to a briefing of SMI Services including architectural views to delineate between:

- Identity Management
- Credential Management
- Attribute Management
- Privilege Management

Concluded that the SC/5 activities covered more than just identity Management.

Discussion points raised by the group included:

- Maturity of standards
- Pace of implementations
- Paradigm shift to information sharing
- Vetting process for below Confidential
- Cross Certification ongoing with Slovakia
- Transitive Trust across NPKI Root Ct

Conclusions

- Both SC/4 and SC/5 work is still in progress. Difficult to make conclusions yet.
- Clear need to harmonise SC/4 and 5 work to a single model + terminology.