



# Federate Locally, Federate Globally

RL "Bob" Morgan  
University of Washington and Internet2  
European Advanced CAMP  
Málaga, Spain  
October 2006

- Federation, micro and macro
- End to end
- Interoperability and flexibility
- Inter/confederation and federation services

### 3 parties interacting

requesting party (aka user)

asserting party (aka IdP), relying party (aka service)

“federation” at micro level happens when

asserting party gives requesting party a token, requesting party gives it to relying party, relying party uses it to establish security properties of requesting party

asserting party and relying party are under separate administration

(note useful case when requesting party and asserting party are the same, ie user asserts about itself)

Federation (at micro level) is a fundamental building-block computing structure like “file”, “network”, “GUI”, “database”, etc hence not product- or technology-specific permits specialization in management of security information

- asserting party can be good at user proofing, authentication, roles, etc
- relying party can be good at stuff specific to its application area

### 3-party federation requires many agreements

what can be asserted about user, both syntactically and semantically (ie, what kinds of things is a particular asserter permitted to assert, in eyes of RP)

information flows at signon time

protection/validation methods for transmitted data

responsibilities of asserting and relying parties

capabilities of requesting party (ie client)

elements specific to parties: integration, usability, error handling, etc

Micro-federation is good, so we want to do it a lot  
ala many files, GUI windows, inter-networks, etc

## Federation at macro-level

supports interests of many parties in doing micro-level  
federation, by creating community to reduce barriers

## Hence

naming of parties, discovery/listing of parties, defining  
use of options, organizing into sets by characteristics,  
establishment/removal processes, etc

primarily about parties benefiting from shared  
management

## 2 kinds of people in the world

those who cling to end-to-end principle, those who don't

## End-to-end argument says

elements interacting via infrastructure are responsible for their own semantics; infra services support/optimize but do not alter

## following this principle in macro-federation

federation infra supports parties in management of info needed for their micro-federation interaction, but doesn't take active part in interaction itself

parties can micro-federate outside of macro-federation

An instance of micro-federation

uses more or less static feature set: user identifiers, encryption, flow, attributes, etc

A macro-federation supports constrained option set

in order to support diversity of business purposes

key issue is expectation (or assurance) of full NxN interoperation

most federations have assumed/mandated this, but it is unlikely to persist going forward (SAML 1 vs 2, WS - Fed, WS - Trust)

managing option evolution is key technical role of fed

## Logout

to some, federated login implies federated logout  
eg federation services tracking/ending sessions  
really supportable?

## role of PKI in supporting SAML interaction

SAML sends signed assertions, TLS-protected services  
should these operations rely on classic PKI (certs, CAs,  
cross-certification, name constraints, key purposes,  
etc) or handle public key operations via SAML-specific  
structures?

## Interconnection among (macro)federations

depends on agreement about (macro)federation function  
can federation-mediated and end-to-end models  
interoperate? we'll find out ...