InCommon and Global Federation Issues

Tom Barton

CISO @ UChicago

Internet2/InCommon

Changes afoot in global federation

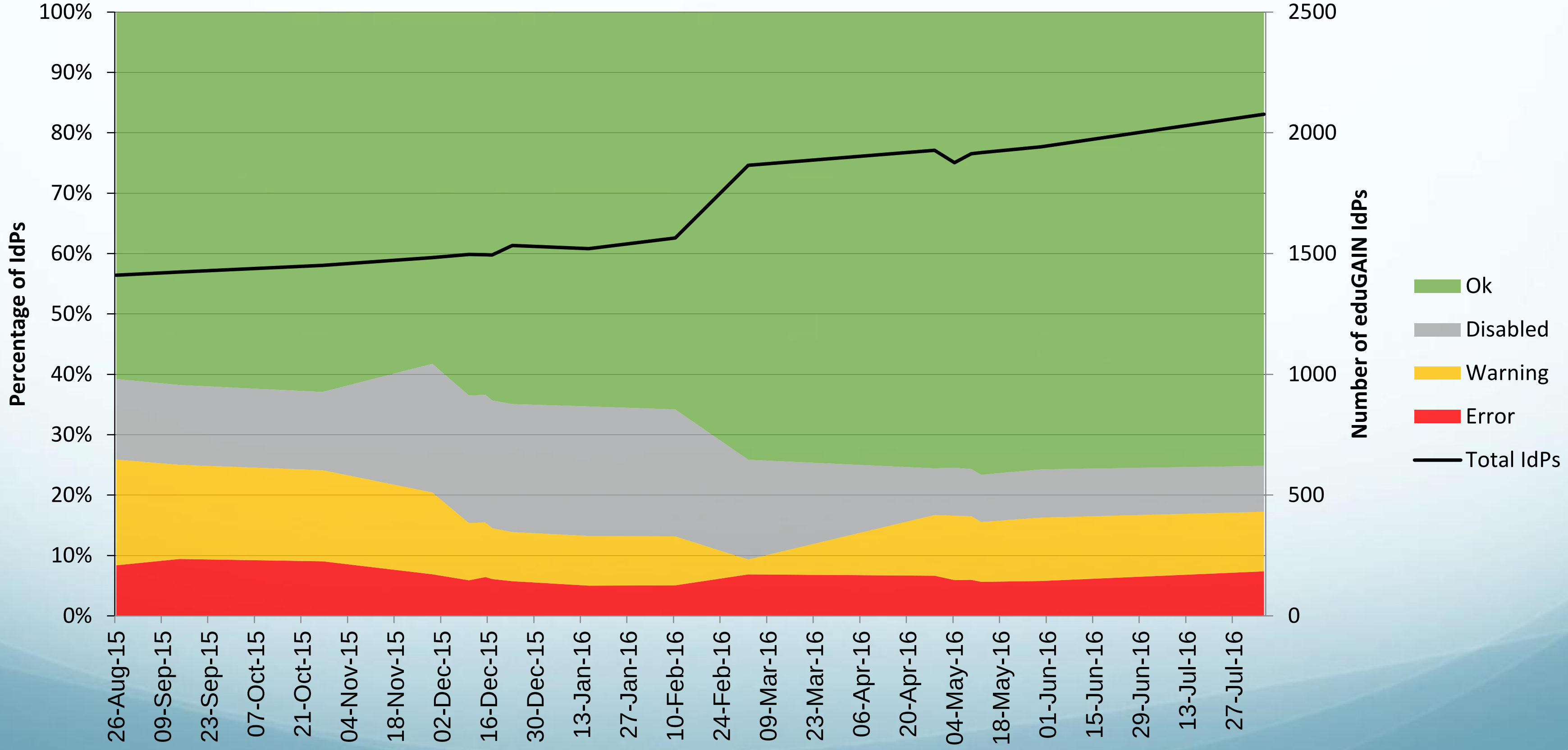
- Scale of global federation and the role of federation operators (fed ops)
- Managing risk of federated authentication
- Elevating trust in federation

Theme:

Maturing global federation demands evolving the roles of federation operators and federation members in producing trust in federation

eduGain stats

IdPs	2227
SPs	1384
Feds	38



Identity Provider Status According to eduGAIN Connectivity Check Service (ECCS)

Maturing eduGain & evolving roles

- Errors in one federation can impact all others
- What should be published to eduGain, what should be filtered from it?
  - Entities: opt-in/opt-out approaches
  - Entity attributes – Entity Categories, Assurance attributes, etc
- Which parts of metadata should federation operators police?
- What autonomy should members have over their own entity's attributes?

➢ ***There is a commons to steward and all parties share responsibility***

Disaggregating metadata

- Global metadata aggregate that fed ops sign is getting too big for some SPs and IdPs
- Bite-sized metadata: MDQ - MetaData Query
  - Fed ops signing workflows to be defined
  - Infrastructure for global MDQ service to be defined
  - Owned & operated only by fed ops?
- Dynamic metadata
  - Federation operators & members both have roles in anchoring trust
  - Proposed for OIDC federation, ideas and processes transcend choice of federation protocol

Managing risk of federated authentication

- Low uptake of FICAM-style Level of Assurance in R&E
  - High cost
  - MFA needs to be separated from scalar LoA value
  - Lacks security incident response
- MFA interoperability
  - Standard for how SP signals that it wants MFA and IdP response
  - InCommon WG defined standard profile
    - Includes work on identifying MFA types that are “good enough”
  - REFEDS working to make it a global standard

REFEDS assurance profile (for research)

- Major research Virtual Organizations were interviewed to understand risks and associated properties needed of federated authentication
- Profile components to be signaled as Vectors of Trust
  1. Identity concept
  2. Identity proofing and credential delivery, renewal and reissuance
  3. Authentication
  4. Attribute quality and freshness
  5. Management and organisational considerations
- Map to scalar values also (“minimal”, “higher”)
- Build on International Grid Trust Federation, eIDAS, Kantara
- Initially complete draft to be presented in November 2016

Sirtfi: federated security incident response

- √ Sirtfi Trust Framework (an assurance profile)
  - Basic security practices each member self-attests to
- √ Standard representation of security contact in metadata
- √ Sirtfi assurance attribute in entity metadata
- √ Fed ops role normatively defined, and modest
- Dutch federation 100%
- Swedish federation about to become 100%
- CILogon, WLCG/CERN
- InCommon pilot, production “real soon now”
  - REN-ISAC WG to be chartered to maintain security contact info
- Increasing global engagement – it’s a Good Thing!

Baseline Expectations for Trust in Federation

- Short list of simple high level statements that are to be true of IdPs, SPs, and Federation Operators. Egs:
  - "The IdP is trusted enough to be used to access the organization's own systems"
  - "Generally-accepted security practices are applied to the SP"
- Finalized within InCommon after broad community consultation
- Implementation plan being developed. Highlights:
  - Amend Participation Agreement so that all InCommon members must meet Baseline Expectations
  - On-going community engagement to ensure Baseline represents community consensus
  - Non-compliance ultimately leads to removal from InCommon
- Future: take it global via REFEDS

Evolving roles for trust in federation

Federation Operators	Federation Members
Anchor trust • Metadata service • Metadata signing • Delegation to members (future)	• Meet Baseline Expectations • Perform delegated roles (future)
Operate processes supporting • Completeness and accuracy of entity attributes • Community review: Baseline, Assurance	• Maintain completeness and accuracy of own entity attributes (part of Baseline Expectations) • Participate in community review (decisions made by those who show up)
Collaborate and partner • REN-ISAC (or equiv outside US) • REFEDS • R&E constituent organizations	• Participate in Sirtfi • Participate in Working Groups (decisions made by those who show up)
Operate value added services	Pay for value added services (in US)