Strong Authentication - side meeting notes from TNC19

Strong Authentication Lunchtime Chat, Thursday 18th of June, 12:30, TNC2019 Tallinn

Attendees:

(apologies for any inaccuracies! Notes by Hannah Short)

- Heath/Bradley: AAF, lots of talk from research communities. Seeing universities deploying MFA for their own internal services.
- Alan: SP, would like to increase assurance level for identities using UniDays.
- Ann: Incommon/Internet2, looking to see what people are doing.
- Miro: Croation Federation, some services would like to have stronger authentication (not very strong request). Also serve schools, who would strongly like a simpler authentication method than password, looking at WebAuthN, FIDO and others.
- Pal: SUNET, kicked off a year ago, one service requires it for medical records. Also strong identity proofing.
- Mischa: Nikhef, Research Community, interested from RCAuth perspective, assurance would help.
- Uros: KIT, Research & EC Projects, just watching
- Jule: Research & EC Projects assurance profiles (sfa), looking at identity vetting for second factor tokens
- Maarten: NREN & EC Projects, would like to understand use cases better
- Jose: Federation Operator SIR, looking into mfa and sfa profiles. Want to understand better where it can fit in hub and spoke federation
- Jaime: UNINETT, maintainer of SSP which should accept and provide profiles. Also FEIDE runs a single, centralised IdP so can offer as a service
- Lars: FEIDE too, see Jaime
- Victoriano: University of Malaga, use cases that need stronger authentication (run internal federation)
- Lucy: Facilitating Fed2.0 workshop. Interested in below-web authN too.
- Leif: ran 2fa in eduID for a while but stopped (partially because insecure). Also difficult to explain to users. Ready to start taking next step towards password free flows. Looking at other ways to get WebAuthN into federations.
- ?: New Zealand access federation
- Peter: Hungarian access federation, interested in technologies and use cases
- Attila: Also Hungary. How to suggest to members to follow best practices. Can we make it compulsory
- Pavel : Slovenian NREN, service for primary schools but getting requests for it
- Dave: Research, chaired group 20 years ago, decided that face-to-face vetting was required. Here for interest
- Sander (?): Builds services for IdPs/SPs, interested in what others are doing
- Scott: Multiple research projects, many would be happy to consume information about strong authentication from IdPs. Want signalling across federations . Many AARC BPA implementations, want to add 2fa
- Tom: Incommon/Internet2 & Research, message that it's necessary to do things in a coordinated way
- Gerben: SURF NREN, Science Collaboration Zone,
- Benn: see Scott
- Brook: Nothing to add
- Arnaut: SURF, looking to support research groups and generally
- Laura: SP ORCID, Spherical Cow group. Still challenging to know how authentication assurance matters when you don't know the person
- John: AAF, looking for real use cases
- Richard: North Dakota State University, hoping to get ahead of the curve
- & 5 extra people who joined later

Notes:

- What is Strong Authentication? Credentials that allow protection against phishing. Credentials where you have to be physically with the person to impersonate them. SMS and OTP methods are questionable today. Let's mitigate the phishing risk.
- Also talking about the processes that go with this.
- Do these things need to be bundled? Strong Authentication & Identity Vetting
- Separation of self protection and organisation protection
- We will not be the first to find out about compromised credentials
- There is a drive from users to improve user experience, e.g. no passwords
- Research Communities, not all want it. Some need to do it already internally. Would like to avoid the case that researchers need to authenticate multiple times with strong tokens.
- Passing the authentication all the way through multiple layers of federated identity
- There are already services doing this, thanks to CiLogon. 1000s of groups. Might be worth trying to track what works.
- Next steps
  - Should this go back through REFEDS?
  - Maybe this can be rolled into a trust and identity hackathon? (Would also bring more technical young people in)
  - Go a step further from MFA profiles, into best practice r.e flows/buttons etc. (there is an Incommon MFA document, it discusses expectations)
  - FIM4R, would be good to clarify what is required and what is the range. Perhaps an architectural document
- Not sure what it is we are trying to do, is this about outreach or best practices? (Laura)
- Could work towards harmonisation of baseline
- Alan to propose a WebAuthN REFEDS WG (suggestion that maybe it should be more generic)
- Q, do we want people to know how to do it, or do we want people to do it?
- We need services to require it
- We will have issues with signalling with commercial vendors

Resources:

- Shibboleth Multifactor Authentication Configuration.
- InCommon MFA Usage Guidance

Use Cases brought up during discussion

- Sensitive services (e.g. Medical records)
- Schools, particularly younger people (easier, not necessarily stronger)
- Some research services (e.g. RCAuth, some SP proxy implementations)
- Services of financial value (e.g. discounts)