AARC-G029 - Guidelines on stepping up the authentication component in AAIs implementing the AARC BPA

Summary

A number of research community use cases require users to verify their identity by using more than one type of credentials, for instance using password authentication, together with some physical object such as a phone or usb stick that generates tokens/pins, etc. At the same time, there are services that may require an already logged in user to re-authenticate using a stronger authentication mechanism when accessing sensitive resources. Authentication step-up is then needed to improve the original authentication strength of those users. This document provides guidelines on step-up of the authentication component. It covers requirements and implementation recommendations, describes a proposed authentication step-up model, and outlines related work and documentation.

Links

Guidelines page

https://aarc-project.eu/guidelines/aarc-g029/

Working docs

Google-Doc: https://docs.google.com/document/d/1lQqK9-_DTRwrqeFhiQywQ0iVZindFrK9-Ozx9eY0ols

Final Documents (MS Word & PDF)

Meetings schedule and Minutes

Date	Location	Agenda	Minutes
2017-07-17-11 13-00 (CEST)	https://webconf.vc.dfn.de/aarc-jra1	Discuss documents A, B, C: • Table of Contents • Key points to mention	We essentially worked inside the documents. Minutes do not make sense at this point

2017-07-28 13:00 (CEST)	https://webconf.vc.dfn.de/aarc-jra1	Discussion of documents A, B, C	Decided to prioritise document C Introduced June from RZG, who is liasing for Geant to consume results of our document Document responsibility handed to Uros, Finalise Intro: Marcus
2017-11-07 10:00 (CET)	Agreed from now on to use Vidyo room: https://www.nikhef.nl/grid/video/?m=aarcjra1	Doc discussion	Short review of the doc, and discussion about the future steps. Discussion about the possible implementations of the step-up: From the SP point of view, there are 3 use cases: ▪ First, if the SP requires having MFA (or step-up of other components), then all IdPs which users are accessing this service need to support and provide MFA, which may be difficult to achieve ▪ Second, the SP itself may implement MFA functionality (the actual implementation of this use case was not elaborated at this point) ▪ Third (most interesting at this point), there can be IdP-proxy that can provide step-up service (e.g. for MFA) Possible description of the third use case: ▪ User authenticates with the SP and establishes a browser session. The SP then can redirect the user to the predefined IdP-proxy service, where the user can then go through the step-up procedure (e.g. perform MFA). After successful performance of the step-up procedure, the user is redirected back to the SP. SP then can grant access to the user. Future work: • Pinging Stefan for SafeShare chapter: Uros • Review old comments and try to resolve them: Uros • Create initial drawing of the third use case, on lucidchart: Uros • For everyone: going through the doc, and fix current issues
2017-12-05 10:00 (CET)	https://www.nikhef.nl/grid/video/?m=aarcjra1	Discuss evolution of SuA documents	There will be **three** documents: 1. **Authentication-step-up:** • Short, concise, to the point (e.g. 4 pages) • Document here: https://docs.google.com/document/d/1lQqK9-_DTRwrqeFhiQywQ0iVZindFrK9-Ozx9eY0ols • Step up for SPs that are connected to a proxy • Based on TNC18 Abstract by Jule and Marcus • Capturing the discussion we had on AARC2-AHM-day3 • This will be the new JRA1.2C document for the deliverable 2. **AuthN-freshness-step-up:** • Like above document, but focused on AuthN Freshness • Document here: https://docs.google.com/document/d/1BgwXppt09Mntfg6Z59BEK5rA0nVN2mZCgF3fHsy2eaw 3. **General assurance elevation:** • "Holistic" document • It's the "old" document that will evolve to the holistic one: https://docs.google.com/document/d/1R24xKC-cC7sLyb13Gr2jxKtlA83_qESrkCorT4PTb74 • All definitions • General assurance elevation on components • ..."make it look like an IdP (from the SP perspective)" • Still keep it to the point. 4. Experiences of the pilot...
2018-01-16 10:00 (CET)	https://www.nikhef.nl/grid/video/?m=aarcjra1	Followup on Step-Up and other documents	We agreed to put all definitions to the AARC1-JRA1-Terms and definitions google doc at https://docs.google.com/document/d/18AllfUKLi90f1odm6hINkQvRljbFhy9lfkY1M447uBQ
2018-01-30 10:00 (CET)	https://www.nikhef.nl/grid/video/?m=aarcjra1	Finalise Step-up document	Received various comments from Mikael, Jens and Mischa Will include step-up flows from a Geant doc of Christos (Second factor authentication component for the Life Science AAI) Will have Session at TIIME to discuss final document Marcus will circulate a close-to-final version on Wednesday
2018-02-13 10:00 (CET)	https://www.nikhef.nl/grid/video/?m=aarcjra1	Finalise Step-up document	Received comments on close-to-final version Discussed comments Marcus will circulate a 'pretty-final' (=closer-to-final) version on Wednesday The call was **missing partners** from ▪ EGI ▪ PSNC ▪ Surfnet
2018-03-06 10:00 (CET)	https://www.nikhef.nl/grid/video/?m=aarcjra1	Finalise Step-up document	Move sections 2 and 4 to appendix Open consultation about the recommendations

2018-03-13 10:00	https://www.nikhef.nl/grid/video/?m=aarcjra1	Finalise Step-up document	Closed final comments in the document. Document frozen for the internal review at Geant (many thanks!!)
2018-03-20 10:00	https://www.nikhef.nl/grid/video/?m=aarcjra1	Finalise Step-up document	
2018-03-27 10:00	https://www.nikhef.nl/grid/video/?m=aarcjra1	Information on finalisation process	Additional recommendation regarding the home-IdP to announce his capability to do MFA added to the document.
2018-04-04 10:00	https://www.nikhef.nl/grid/video/?m=aarcjra1	Information on finalisation process	We had further discussion on the document over easter. In addition to wording, changes were mostly regarding whether and how the home-IdP announces his MFA capability. This part was moved to conlcusions, because it's not quite clear yet. We also discussed whether we recommend that IdPs SHOULD inform whether they have MFA or whether they HAVE TO (in the sense that it would not make much sense otherwise). We agreed on SHOULD.