Evaluation of possible LS AAI pilot solutions and formal recommendation

Suggested way of evaluating:

- We rank requirements using MOSCOW.
- Then rank the solution with:
  - Green: fits requirements, possibly after configuration
  - Orange: may be supported, but needs coding
  - Red: not supported, or needs major coding
  - Yellow: Open Questions
- We then count MUST/SHOULD/COULD amount of green/orange/red
- Some specific questions are not part of evaluation (which is then mentioned)

1. Evaluation

Requirements	OpenConext Stepup	CSC MFA Service
1 Architecture		
1.1 Please describe the high level architecture, flows and components used in the	SAML2 proxy or SAML2 SFO	SAML2 proxy and OIDC OP to interact with clients Architecture supports three main use cases: 1) SP requests 1FA and 2FA from MFA proxy

proposed solution **NOT PART OF EVALUATION**	Flows for login, second factor registration and revocation, Registration Authority see: https://github.com/OpenConext/Stepup-Deploy/wiki/Application-Flows	2) SP requests authentication from IdP. IdP authenticates the user with first factor, then IdP exploits MFA service for 2FA. 3) SP first exploits IdP for 1FA, then MFA service for 2FA.
1.2 Please describe which and how the high level requirements are met in the proposed solution		
1.2.1 The service should be integratable in existing environment in a standards compliant way **MUST**	SAML2 web SSO profile internally & externally REST APIs, see: https://github.com/OpenConext/Stepup-Gateway/blob/develop/docs/GatewayAPI.md and https://github.com/OpenConext/Stepup-Middleware/blob/develop/docs/MiddlewareAPI.md	✔
1.2.2 From the point of view of a Service Provider, the service should behave as a SAML2 IdP. **MUST**	✔	✔
1.2.3 Users should be able to login to the service using their eduGAIN or community IdPs through the Northbound proxy **MUST**	✔	✔

1.2.4 Users should be able to register and manage their tokens/devices **MUST**	✔ (Self-service component, web interface)	✔
1.2.5 Integration with Service Providers should be possible using either SAML or OIDC **SAML MUST, OIDC SHOULD**	SAML only (OIDC planned this year)	✔
1.2.6 User should be able to authenticate using a pre registered token **COULD**	API available	**X** (Solution can be extended to 6 and 7)
1.2.7 Next to self registration, it should be possible for a Collaborative organisation to register the user. **COULD**	API available	**X** (Solution can be extended to 6 and 7)
1.2.8 What is the delivery model of the proposed solution? (as a service, buy, software package?)	- Open Source - Ansible playbooks - As-a-service or installed at an institution	- Open Source - Ansible to deploy the solution - As a service and may be taken also as it is

Open Source MUST **Ansible SHOULD** **or eq. MUST**		
1.2.9 Is a demo service available for testing? **SHOULD**	✔ (public Stepup installation as a service for pilot purposes, OpenGini IDP to register accounts)	**X** (https://rr.funet.fi/mfa2.html test page for production service. No demo site as such as you need verified sms numbers)
1.3.0 Please describe what information must be permanently stored by the service to function properly **Data Minimization MUST**	- user identifier (SAML Subject NameID) - user common name - user institution (schacHomeOrganization) - user email - information required to use the 2nd factor (phone number for sms, token id for Yubikey) → mechanisms that allows PII to be removed - vetting process: last six digits of identity document - registration authorities and vetting locations are stored by the service - information of connected IDP proxy and connected SPs	- key of the user (encrypted format) - token secret (encrypted format)
2 Core Features & extensibility		
2.1 Authentication		

2.1.1 Please describe which Open Standards are supported for authentication **SAML MUST** **Other SHOULD**	- For SPs: SAML 2.0 - new second factor types can be added using Generic-SAML-Stepup-Provider - Second factors based on U2F and Yubico cloud API - Tiqr uses OATH OCRA protocol	- SAML2, proxying use case. All profiles which are supported by Shibboleth IdP. - OIDC provider, currently implicit flow. Authorization code and hybrid flows will be supported once GEANT4-2 Task 3 finishes the implementation work.
2.1.2 Please describe if the solution can be used as a proxy by itself (so for SPs connected directly to the Stepup gateway) **MUST**	✔	✔
2.1.3 Please describe if the solution can be used as a Second Factor only Identity provider **SAML MUST** **OIDC COULD**	✔ (only SAML)	Second Factor only OIDC OP, may be extended to Second Factor only SAML2 Identity provider
2.1.4 Please describe if the solution supports additional non open standards APIs for authentication **COULD**	✔ (Microsoft ADFS MFA extension using SFO interface)	**X** (only SAML2, OIDC are supported)

2.1.5 Does the solution support REFEDs MFA? **SHOULD**	**X**	✔
2.1.6 Does the solution support other LOA frameworks? **SHOULD**	- NIST SP 800-63-1 / ISO 29115 LoA levels 2 and 3	**X**
2.1.7 Does the solution allow adding new LOA frameworks, and if so how? **MUST**	- Changes in the workflow, implementation required - Changes in the binding of identifiers to LoA levels, no implementation required	Authentication context classes may be used to define acceptable combinations of authentication methods. New methods may require building new adapters.
2.2 Second Factors		
2.2.1 Please describe which tokens are currently supported **2 MUST**	- SMS (native, via MessageBird API) - YubiKey (native, via Yubico cloud API) - Tiqr (via GSSP) - U2F (native)	- SMS - TOTP - Email SMS is currently expected to be injected from a trusted source that has done the identity vetting of the device already in a trustworthy way. (in this case HAKA Institutional IdP). This methodology is known not to work for Elixir in it's current form. TOTP is implemented as a delegated token based on

		top of SMS. Hence it is not stronger then SMS. The vetting of the TOTP also does not mandate the use of the same phone as was used to register SMS, so it might be that the token is (still) in use after the user lost his.her phone. Email is sending a one time token to a email box. As such it is not a second factor, but only proof of access to the mailbox.
2.2.2 Please provide an indication of the cost associated with the use of the tokens as described in 2.4 **NOT PART OF EVALUATION**	- SMS (about 0,06€ per SMS, depending on volume) - Yubikey: price of token (Starting from 30€, depending on volume) - U2F: Price of token (many choices, many quality and security levels, hardware based U2F tokens cost about 15€) - Tiqr: requires a iPhone or Android phone. (Tiqr server components are open source. You should expect to host there yourselves if you intend to offer Tiqr)	- SMS: 0,09€ (Twilio which is now supported) - TOTP: free of charge - Email: free of charge
2.2.3 Please describe which Open Standards are supported for integrating with tokens **SHOULD**	- U2F - GSSP	- New tokens require a adapter to be created for the service
2.2.4 Please describe if the	- Yubico cloud API	- New tokens require a adapter to be created for

solution supports additional non open standards APIs for integrating with tokens. **COULD**	- MessageBird API (SMS) - Tiqr: API of Apple and Google for sending push notifications	the service
2.2.5 Please describe how to enhance token support - How can new tokens (new forms of second factors) be added to? **NOT PART OF EVALUATION**	- GSSP, method based on SAML 2.0 for adding new tokens in a generic way (see: https://github.com/OpenConext/Stepup-Deploy/wiki/Generic-SAML-Stepup-Provider)	- Solution may be extended to support any token supported by Shibboleth IdP such as Duo Security and U2F. Any other token can be supported with appropriate adapter.
2.3 Identity Vetting		
2.3.1 Please describe how identity vetting is supported **SHOULD**	✔ (Face-to-Face check using Stepup RA component, allows delegated identity vetting, web interface for vetting process)	**X** (not supported)
2.3.2 Is self registration of tokens supported? **MUST**	✔ (registration of tokens using self service, in order to use token identity vetting is mandatory)	✔ Tokens can be self registered. Additional policy rules can be used to limit self registration to certain tokens or use cases

2.3.3 Please describe how new identity vetting flows be added? **SHOULD**	- requires coding	Depends on vetting procedure itself. If vetting would require participation of the MFA service itself a new flow would be configured to it. More likely scenario would be vetting performed outside MFA service resulting in tokens read by MFA service.
2.3.4 Please describe if an API is available for adding new vetting flows? **COULD**	**X** **API itself is there, but new flows also (likely) need new business logic which needs config and/or coding (see 2.3.2)**	**X**
2.3.5 Please describe if an API for starting identity vetting from an external application is available **NOT PART OF EVALUATION**	**X**	**X** (User that needs to be vetted by external application may be directed to external vetting if such service is defined)
2.3.6 Please describe what information (attributes) are required for identity vetting **NOT PART OF EVALUATION**	- common name - email address - EPTI	**X** (Vetting is not part of the core service)
2.4 User Interface		

2.4.1 Can the UI be branded per community/customer? **SHOULD**	Branding per installation possible	✔
2.4.2. Does the UI support internationalisation of content and messages? **SHOULD**	✔ (English, Dutch)	✔
3 Security		
3.1 Please describe the design security considerations	- Separation of duties between components (Only middleware can write to databases, only selfservice and RA can access middleware, through REST API, only RA can vet, only self service can register a new token, Gateway handles all authentication, Self service as well as RA and Gateway have readonly access to database: gateway has its own database with only active tokens as well as users and IdP/SP configuration) - Segregation (Stepup Components run as different users using php-fpm, Tiqr OATH secrets can be managed by a separate key server)	Solution is built on top of Shibboleth IdP framework, relying on it for SAML2 communication for both SP and IdP interfaces, trust achieved with standard Shibboleth mechanisms. For OIDC interface a client with client id, redirect uri and request signing keys must be registered to be used.

	- Detection: Event sourcing means that there is a complete audit trail of all changes to the state of the system - Centralised logging: Log messages from applications are generated with central logging and analysis in mind. See: https://github.com/OpenConext/Stepup-Deploy/wiki/Logging-Strategy - Ansible playbook: Separation between OS roles (require root) and Stepup component installation (do not require root) and component configuration through REST API (cannot modify / read system)	
3.2 Please describe the development security considerations	- Code audited periodically - Deployment pentested - peer review for commits - reuse existing components (e.g. saml2 lib from simplesamlphp) - Symphony2 components like nelmio/security-bundle to defend against common web application vulnerabilities	- Peer code reviews are used - Security trainings for developers
3.3 Please describe the operational security consideration that need to be put in place to securely deploy the solution	- Ansible script as starting point - Manage infrastructure: configure host firewall, VLAN ACL, protect management access to servers, monitor - Create backups - Pentest, audit	Solution is hosted in data centres that have been granted an ISO/IEC 27001 certificate for their information security management systems. ISO/IEC 27001 standard, ensures that the organisation possesses the capacity to manage, govern and continuously develop the

NOT PART OF EVALUATION		information security of its services and operations.
3.4 Please describe which measures have been implemented to protect personal data in the solution **MUST**	- Removing PII: “Right-to-be-forgotten”	- TOTP key and key identifier are both stored to database in encrypted format. - No unencrypted/plaintext data is stored.
3.5 Please describe if the solution and/or its software has been audited by external Security Audits. If so, are the results available? **SHOULD**	✔ (two audits, another this year, no digital copies of results allowed)	**X**
4 License		
4.1What is the license of the solution, if relevant **MUST**	- Apache 2.0	- https://opensource.org/licenses/MIT
4.2 Who owns the IPR/copyright?	- SURFnet B.V.	- CSC - IT Center for Science, http://www.csc.fi

NOT PART OF EVALUATION		
5 Support and Development		
5.1 Roadmap		
5.1.1 Please describe the roadmap for the solution for at minimum 1 year in the future	- Support for more than one active token per user - OIDCt support (this means adding SFO support to https://github.com/OpenConext/OpenConext-oidc, not adding OIDC to the Stepup-Gateway) - Deprovisioning of users, revocation of tokens that have been inactive for a set time - Improvements to SFO integrations with external systems (Microsoft ADFS, F5 BigIP, Citrix, others) - Pilots with remote vetting (i.e not face-2-face vetting) - Pilots with Context-based authentication - Reuse of tokens from commercial vendors (e.g. institution is using (on premise) Vasco, RSA, … tokens) - Adding additional second factor tokens (U2F (improvements, code is already present but disabled in production),IRMA (using GSSP),Proof	- Implementation of fine grained policy rules for configuring multi factor authentication to apply in certain use cases

	of Concept: Microsoft Azure MFA) - Security audit see also: https://wiki.surfnet.nl/display/surfconextdev/Roadmap https://www.pivotaltracker.com/n/projects/1163646	
5.1.2 Please indicate the projected development budget for the realisation of the roadmap	- different budgets (internal, external) - Budget not the restriction --> Time/people - SURFnet: 3 people available for development -	**X**
5.1.3 Please describe how development of the solution is funded/sustained	-	- Finnish higher education identity federation Haka funds solution development - Finnish Ministry of Education and Culture supports parts of the solution development through MPASSid project - OpenID Connect parts of the solution are funded through GÉANT 4-2 Task 3 (TrustTech)
5.2 Deployment		
5.2.1 Please describe (high level) how the solution is installed	- Ansible playbooks and scripts	- Automated provisioning scripts (Ansible) are used to deploy the solution

Automated Deploy = MUST		
5.2.2 Is a demo deploy available to test? **SHOULD**	(5.2.1 can be used to setup a demo, demo (pilot) installation for constituency, OneGini to register token) https://selfservice.pilot.stepup.surfconext.nl/	(yes, for Haka users) https://rr.funet.fi/mfa2.html
5.3 Support		
5.3.1 How is support on the solution organized **SHOULD**	- support of installation to its users - OpenConext Support Letter - (Any other (formal) support by SURFnet, outside the OpenConext Support Letter, for your project will have to be explicitly agreed upon)	- Handled as part of Haka federation support
5.3.2 If relevant, is there a Community of users around the solution **SHOULD**	- Stepup is part of OpenConext, which is the vehicle to support the community around all OpenConext projects	- Haka IdP administrators exchange information how they adapt use case 2. - The solution has also been presented and discussed in the Finnish higher education IAM special interest group.
5.3.4 Please describe support for integrators wanting to use the solution	- For open source use: OpenConext Support Letter, OpenConext mailinglist for support - For integrators to use SURFnet hosted	- Trainings for both SP and IdP admins - Haka help desk also offers support

SHOULD	solution: support@surfconext.nl, documentation in wiki	
5.3.3 Please describe support for token vendors wanting to add their tokens to the solution **SHOULD**	- Open to new tokens using GSSP API - see also 5.3.4	- May adapt any API provided by token vendor or support 3rd party by providing a interface for the token module.
6 Showcases		
6.1 Please describe a showcase where the product is in use in a production setup **PROD = SHOULD** **PILOT = MUST**	- Best practice: VU University Medical Center Amsterdam: 2nd factor against data breaches (in Dutch) - Best practice: Avans University of Applied Sciences: Creating and managing assessments with an additional security check (in Dutch) - Best practice: Inholland University of Applied Sciences: Marks recorded more securely through two-stage authentication (in Dutch)	- Haka identity federation
6.2 Describe at least two production use cases that are being met with the solution **SHOULD**	- VUmc (VU University Medical Center) uses SURFconext Strong Authentication for remote access to their Citrix Remote Desktop. They are using the SFO API of the Stepup-Gateway - University of Amsterdam uses	- Proxy use case where solution is used to protect remote desktop for sensitive material use. All authentications are handled through solution. - IdP integrated use case where security service requires multi factor authentication. When service in question requests authentication, IdP

	SURFconext Strong Authentication to protect access to several services (Figshare (sharing research data), SAP (enterprise resource management), Testvision (digital tests))	requests multi factor authentication.
6.3 Describe the amount of use (institutions/transactions) for the production instances of the solution **SHOULD**	- Nine institutions using the service (january 2018), these have a total of 13500 active tokens, and did a maximum of 4269 logins per day in december 2017 and had an average of 1927 logins per day in december 2017.	- Four organizations in the Haka federation are using the MFA service in production
6.4 Describe which tokens are used in the production scenarios **NOT PART OF EVALUATION**	- Tiqr - YubiKey - SMS	- TOTP - SMS - Email

2. Formal Recommendation

2.1 Highlevel comparison

The products were compared using MOSCOW, assigning points for every MUST, SHOULD or COULD criterium. If a product does not meet MUST or SHOULD requirements the impact is discussed. If a criterium needs additional work, it is also discussed.

Requirements	OpenConext Stepup	CSC MFA Service
MUST	17	15
SHOULD	12	6
COULD	4	2

At first glance, it is clear that OpenConext Stepup is a more feature rich product, with better support for the MUST, SHOULD and COULD features requested.

2.2 GAP analysis

This GAP analysis zooms into impediments that may come from unmet requirements and discusses the impact. Next we evaluate features that are missing but should probably be implemented in a reasonable amount of time.

2.2.1 Unmet requirements

The OpenConext product does not have any unmet requirements.

The CSC MFA Service does not meet the below requirements

2.2.1 Please describe which tokens are currently supported (MUST)
The CSC MFA Service product currently support 3 types of second factors: SMS, TOTP and email.

- During the discussion, it has become clear that the use of the email token is in fact not a second factor, but consists of sending an email with a confirmation token to a well known domain, for example that of a member institution of a federation. While this feature is convenient to allow a user to prove ownership of an email account, it is not a second factor as such as it is very likely the first factor used for federated authentication is the same as the credential needed to gain access to this mailbox. In addition, the trust in this token is only usable within the context of a federation policy, and hence does not work well for the scenarios where collaborative organisation work across federation and national borders.
- SMS as such is known to be a rather weak second factor. Key in the use of SMS is the binding of the mobile device and the telephone number to the user. Currently the CSC MFA Service does not have the means to make this binding in a secure way. Instead, it assume the institution issues a mobile number through an attribute from the IdP for the user and has done the binding in an acceptable manner. While this works well in the context of a national federation where access is only needed to services of the institution itself, it is unclear how that would work for a collaborative organisation. It is very unlikely all institutions participating in a collaboration will or even can deliver a mobile number as part of the authentication. Also a generic, globally accepted policy for binding the number to the user is missing.
- The TOTP solution offered turns out to be vetted based on SMS. In the first step of vetting the TOTP, the SMS factor is used to bind the TOTP to a device. Because of this, the TOTP factor is not stronger then the SMS token and suffers from the same challenges as reported for SMS above.

Based on the above the unfortunate conclusion is that none of the tokens offered currently in the CSC MFA Service are useable as a second factor solution for a collaborative organisation. The only possible scenario could be were a self asserted phone number is used to bind a mobile number to a first factor. This constitutes only a very small improvement on top of the first factors. As was learned during the discussion with the team from CSC, this use of SMS is not sufficient for Elixir.

2.2.2 Please describe how identity vetting is supported (SHOULD)
The CSC MFA Service product currently does not support identity vetting in any way. As was learned during the discussion with the team from CSC, a few TOTP tokens were manually added to the service database on behalf of Elixir for well known Elixir staff. In effect this is a low level Registration Authority activity. Combined with the support for tokens as described in 2.2.1 this makes the implementing the CSC MFA Service a challenge to implement in a scalable way.

2.3 Requirements that need work

Several requirements in both products are not yet implemented. The OpenConext solution is based on PHP, the CSC MFA Service is developed in Java.

Below is a list of the missing features, the MUST requirements are discussed in more detail.

OpenConext Stepup	CSC MFA Service
2.1.5 SHOULD	1.2.6 COULD
2.3.1 SHOULD	1.2.7 COULD
2.3.3 COULD	**2.1.3 MUST**
3.4 MUST	2.1.6 SHOULD
5.3.3 SHOULD	2.2.3 SHOULD
	2.2.4 COULD
	2.3.2 SHOULD
	3.4 MUST
	3.5 SHOULD
	5.3.* SHOULD

As described in 2.1.3, the CSC MFA Service currently does not support a SAML interface to act as a Single Factor only IdP. This is a MUST have requirement as it is the prefered way we would want to implement our LSAAI solution, so this presents a clear impediment. CSC indicated adding this should not be mayor effort however.

Requirement 3.4 is a MUST have requirement not met by either product to is full extend. While both solution implement some measures to protect PII, it would be a mayor improvement it both would also implement each others features in this field.

Finally, both products need adoption in case new tokens and of vetting flows are added. In both cases the business logic for handling a new token and how that then translates into a specific LoA needs to be added through coding. In case of the OpenConext product several generic and open APIs exist to add new tokens, wheres for the CSC MFA Service all of this needs to be developed in the form of plugins.

2.3 Conclusion

Based on the comparison conducted, the OpenConext Stepup solution is prefered. The product supports more features out of the box and appears to be much more mature, both in support of tokens as well as in support. Only impediment noted is the fact that the OpenConext Stepup solution currently always assume the availability of an RA. In the most simple scenario we want to implement, registering a token as such should already yield some LoA, even though a very low one. From the perspective of the product this constitutes adding a new vetting flow for which we can leverage the available API.

Major challenges identified with the CSC MFA Service product is that it currently does not support any token we would be able to use. Next to this extending the product with new tokens would require coding new plugins. In addition no interface or procedure exists for token binding and identity vetting in any way.