[Public] Questions from the Webinar

#	Question	CSCS Response
1	How can an application on the client machine that interacts with the cluster via SSH and requires long term connections to manage jobs (lasting for weeks or months), to run without crashing and without requiring a human intervention every 24 hours?? This is a compulsoruy requirement for my workflows to run properly.	long term validity keys are available for certain use cases, but for programmatic clients accessing CSCS infrastructure we recommend using FirecREST which is a RESTful API intended to do exactly that.
2	Why shouldn't the user just generate their own private key on their own machine, and just send their public key to CSCS for signing? If the private key was generated in any place other than the user's machine, we lose nonretractability. Plus, if a key ever leaks, we can't know if it leaked from a user's machine or from CSCS itself (even if the key is theoretically never saved in CSCS)	We would like to start in this way as part of our MVP1. But we have some additional plans in our pipeline to enhance this in our MVP2. Please stay tuned.
3	What kind of information is collected by Authentication App about user? How this information is processed by private companies providing the App? Do Microsoft/Google all providers accept Swiss data protection law (e.g. servers being located in the country)?	To install the authenticator app, we need to sign in to Apple Store or Google Play store But to import the seed into the authenticator apps we don't need to sign in to these apps. As far as we know, The cscs username is the data that is embedded into the QR code Example Data: otpauth://totp/**CSCS:nchalla**?secret=KBXXXXXXXXYYZY&digits=6&algorithm=SHA1&issuer=CSCS&period=30 one is free to use whatever authenticate app that one chooses. For example, open source and non-google are available such as Aegis (https://getaegis.app/) As Switzerland eIAM is already going with the Google/Microsoft Authenticator apps, We assume we are also aligned with Swiss data protection law but shared your concern with our Cyber Security team for a review, Access https://feds.eiam.admin.ch/adfs/ls/ & Click on "CH-Login (eGovernment)" Reference: https://www.eiam.admin.ch/r/P/_3282329220_CH-LOGIN_2FA_Auth_EN.pdf?t=1656413785
4	How do you copy a file from local machine to e.g. Daint? We used ssh-tunnels before through ela, but how this process change now? Will you provide short scripts/aliases that people can use in their .bashrc files?	SSH technology is unchanged, therefore, tunneling is possible in the same way. Once a connection is established with a signed key it won't be closed after the expiration of the key allowing copy of files exceeding 24h.
5	does the phone have to be connected to internet? or simply to the phone provider?	If the Authenticator app is already installed on the phone, the Internet is not required for importing the seed or obtaining the OTP.
6	To manage our workload, we have scripts that run over ssh during the night to download data from Daint. Could it be possible to still do it even with the MFA on?	Yes, the SSH Key is valid for 1 day (24h after the date of creation) but for some special cases, we can grant a long-term key that is valid for 1 year but is limited to an IP address. We recommend using FirecREST API to program access to the infrastructure.
7	We use a service account to regularly export Slurm usage for the UZH projects that share a quota. Can you help me to understand (1) is this account part of the MFA roll-out, and (2) if so, then on what date can we expect a switch?	Service Accounts are exceptional for MFA / SSHService.
8	Are there plans to support WebAuthn as MFA method?	We wish but not at this time. (It's there in our long-term goals)
9	Is Microsoft authentication app supported?	Yes we tested that in our environment and it works as normal but please note it was not certified with keycloak.
10	Is the sshservice already live? I am not getting any response from the webserver.	It will be opened to the Internet starting 6th December but only the users who got the invitation email can log in to the SSHService.

11	If one has lost their phone, how do they log into ticketing without multi-factor to submit a ticket?	We are thinking of the following three options but not finalized yet, 1. Send an email to our dedicated email address to reset OTP or disable MFA. 2. Jira will not be enabled with MFA. 3. Login with recovery codes. (TBC)
12	Do you still have to enter a code from Google Authenticator even when doing SSH with the keys acquired from CSCS?	After acquiring the keys no need to enter a code from Google Authenticator
13	When will it come into place?	Targeting to finish enrollment of all users by end of Q1 2023. The Rollout is based on incremental batches and the start date is under review as there are still some config changes required to make on our vClusters. So far sshd config changes were made on ela, daint, dom.
14		
15	Does this affect running jobs on CSCS via Unicore in any way?	As of today, we are not changing the authN workflow for Unicore.
16	Thank you Narendra, does anything change for us if we are already using FirecREST to access CSCS?	Today, no if you already have generated the clientid/secret. To create clients which help in accessing FirecREST API the pre-requisite is users need to log in to our Client Registration portal. And if a user is already enrolled for MFA he will go through the 2FA process to log in to client registration portal. Also, we are working on a solution where we can enhance clientId /secret authentication security to generate an access token which can be compliant with MFA.
17	This solution is not really secure as the passphrase is still not password protected. And what about yubikey or other hardware token used to store the authentication key ?	As highlighted in the webinar, we are highly recommending to set a passphrase immediately after downloading the keys from the SSHService. Besides, we have additional features in the coming version of SSHService (Say MVP2).
18	(I missed the first part of the presentation, sorry if it was already said) - how long does the ssh key lasts? Can it last for at least 1 week? - And from when MFA will start to be implemented/enforced?	Yes the SSH Key is valid for 1 day but for some special cases we can grant a long term key that valid for 1 year but limited to 2 IP subnets. Targeting to finish enrollment of all users by end of Q1 2023. The Rollout is based on incremental batches and the start date is under review as there are still some config changes required to make on our vClusters. So far sshd config changes were made on ela, daint, dom.
19	Hi, so if I understand correctly the MFA is needed only to connect to ela, then to go to daint or eiger nothing has changed?	That's correct, you need to use ssh-agent to propagate the key as described I the documentation.
20	How does the ssh key get set up on the remote host? Is it set up there because it shares my home directory with my local host?	The configuration is using SSH certificates. The ssh key is not needed on the remote host anymore.
21	As a user of user of Unicore with a Service account. Would this affect it in someway?	As of today, we are not changing the authentication workflow for Unicore.
22	Thank you very much for the presentation. What is the expected time where all users will authenticate in that way?	Targeting to finish enrollment of all users by end of Q1 2023. The Rollout is based on incremental batches and the start date is under review as there are still some config changes required to make on our vClusters. So far sshd config changes were made on ela, daint, dom.
23	Following up on previous question: Is it still possible to forward the connection from Ela to compute systems, as previously, using ssh? (by putting ProxyJump in the ssh config file)	Yes possible, SSH capability is not changed, in fact, we selected this method to minimise disruption in the way SSH is being used.
24	is the agent necessary? are the keys needed to ssh from ela to daint or eiger?	ssh agent is recommended but is a user consideration to make your workflows easier. yes you need the ssh key to ssh from ela daint/eiger
25	You mentioned FirecREST for workflows. Does Unicore also work?	As of today, we are not changing the authentication workflow for Unicore.

26	How does MFA interact with services like Globus Transfer?	On accessing Globus through browser and if users select CSCS for the first time then users needs to authenticate with username /password and MFA (Assuming users already enrolled for MFA)
27	If I forget my phone at home and make a ticket, how long will it take to grant a temporaly limited MFA-disabled access? (E.g. if it is just for the day)	I wish we could grant access in quick time say less than 2 hours. (But there should be a cap, say max 3 times per month (TBC) assuming users don't forget the phone every day)
28	For FAQ #1, would it not be better for security to say that users have to reenroll for MFA if they don't have their phone?	yes, it would but we are working on a flow that can also help users to automate the reset OTP functionality without going through the Service Desk.
29	Will I need the additional MFA for FirecREST authentication or for client registration?	To create clients which helps in accessing FirecREST API the pre-requisite is users need to login to our Client Registration portal. And of course, if user is already enrolled for MFA he will go through the 2FA process to login to client registration portal. Also, we are working on a solution where we can enhance clientId /secret authentication security to generate an access token which can be compliant with MFA
30	Can the duration of a submitted job be longer than the time of the session?	if you mean, can the duration of the submitted job be longer than the validity of the key? yes it can. Once a connection is opened, it is not closed after the expiration of the key.
31	How will the access with clients like WinSCP work in the future?	Currently WinSCP do not support this type of ssh keypair. On Windows you could use directly to scp command from the OpenSSH suite, in that case the ssh keypair is supported.
32	when do you expect that all accounts will be migrated to MFA?	Targeting to finish enrollment of all users by end of Q1 2023. The Rollout is based on incremental batches and the start date is under review as there are still some config changes required to make on our vClusters. So far sshd config changes were made on ela, daint, dom.
33	(as a follow up, I see you mention 1 day - can this be increased to 1 week? If I have scripts checking the execution of workflows and resubmitting new ones as needed, I would like that this continues working, e.g., over a long weekend or if I have to take a few days off, without me having to go back to my computer and adding a code once a day)	The cron jobs which are configured on login nodes or compute nodes will not effect, Only if users need to log in to the login / compute nodes then a new key after 24 hours. Whereas if your application pushes some scripts through ssh every now and then, please write to us we will provide a long-term key but Limited to an IP.
34	Is it possible to get a USB-Keylogger?	(i assume you mean a hardware authentication device): it is possible, but not planned for MVP1
35		
36	Employers have to provide the means for employees to do their work by swiss law. So I agree with the problem of private phones. CSCS should not expect people to use private phones as stipulated.	it is not required to use the personal phone. you can complete the authenticator step on the laptop (not recommended), or in the future (MVP2) it might be provided a hardware device for this step. Note that this question if for the employer not CSCS (unless you are a CSCS/ETHZ employee).
37	Will this webinar be uploaded to your site? So that we can see it again when we have to do the installations?	yes, This webinar will be uploaded to one of our public forums along with the questions and answers.
38		
39	How much of my private information is encoded in the QR code that is used to seed the OTP app?	As far as we know, The cscs username is the data that is embedded into the QR code Please refer to #3 for additional info.
40	Can we organize a votation on how long the duration of validity of the key should be ?	No, this is a decision of CSCS to secure access of the research infrastructure funded by the Swiss government. CSCS is accountable and therefore the decision its is own. The duration of validity is under consideration and also we have additional features to enhance this in our coming version of SSH Service (Say MVP2)
41	Do the pilot users already know they are pilot users?	Yes, After our presentation in CSCS User Lab Day some users came forward and subscribed for this pilot launch.
42	What if we have a DHCP implemented for the automatic workflow connecting through SSH and thus cannot use the 1year long key?	The long-term key needs to be created with up to 2 IPv4 network ranges and up to 2 IPv6 network ranges, sufficient to cover most organizations' IP ranges.

43	Concerning the time. Can you confirm it starts 1st of Januar. Also what is the expected duration for the migration?	The Rollout is based on incremental batches and the start date is under review as there are still some config changes required to make on our vClusters. So far sshd config changes were made on ela, daint, dom.
44	Is globus authentication to be done also with mfa?	Yes, If we are accessing Globus through the browser, we need to authenticate using username/password/otp.
45	Given repetitive identical requests, an option could be to implement a ‚Äòone-week‚Äô duration by default, and reduce this time afterwards if anything goes wrong. What about this proposal?	Yes, This is under consideration, and also we have additional features in the coming version of SSHService