



David Groep, 49<sup>th</sup> EUGridPMA meeting  
May 2020

# Legacy DutchGrid CA our BC/DR case



# DutchGrid CA services

Nikhef operates:

- Legacy DutchGrid CA (Nikhef MS): air-gapped classic authority
- DCA Root: air-gapped operation under the classic authority profile
- RCauth.eu: pilot-ca1.rcauth.eu (nikhef instance) online IOTA

*the DCA Root is there only to sign the RCauth ICA*

## What stayed the same: the CA itself has no issues

- repository services of all CAs, and the signing component of the RCauth.eu CA, are all hosted in the Nikhef data centre, location 234b
- air-gapped elements are in a closed room adjacent to it
- network links and routing equipment distributed over two rooms (234b and H140), with on-campus peerings (SURFnet, TENET, KIAE, ProLo)
- NikhefHousing hosts another 185 IP networks (PeeringDB) of which ~15 T1 transit carriers, and is thus Designated Critical Infrastructure
- and the CA, as part of the national e-Infrastructure supporting critical research, in addition is itself important enough
- in either case, continuity in case of lockdown is ensured by joint staff

# What changed

Even if the CA itself continued to operate fine, our users and user organisations may not:

- this has no impact on RCauth, since it's fully federated & automated
- the legacy CA relied on in-person physical meetings with a distributed network of RA agents, and facsimile submission of documents
- fax machines were already become rare in organisations, and are absent in home offices
- the RA agent network breaks down if meetings get cancelled



so for these we devised an alternative, inspired by Jens' call for action

# Part 1: remote submission of documents

We really don't want personal data sent by email, and we want to have as few data as possible on-line (the main audit-log is off-line paper based)

- use a secure file transfer service – FileSender by SURF in this case
- FileSender voucher mechanism implicitly re-confirms control of mailbox
- by re-use of the encryption feature using a secret sent to the applicant by phone/sms, this RA check can even be re-done if desired
- transfer of documents itself is ephemeral (auto-delete), and after printing by the CA operator, the data can be destroyed
- the time limit can be set by the uploader as well

# SURFfilesender voucher mechanism



Preferred language English

Upload **Guests** My Transfers My profile Help About Privacy Log-off

A Voucher allows someone to send you a file.  
To create a voucher, enter an email address then select Send Voucher.  
An email will be sent to the recipient with a link to use the Voucher.

From : davidg@nikhef.nl

To :

Subject (optional) :

Message (optional) :

Expiry date:

**Guest options**

Can only send to me

Advanced settings

**Created transfers options**

Notify me upon downloads

Include me as a recipient

Get a link instead of sending to recipients

Advanced settings

**Guests**

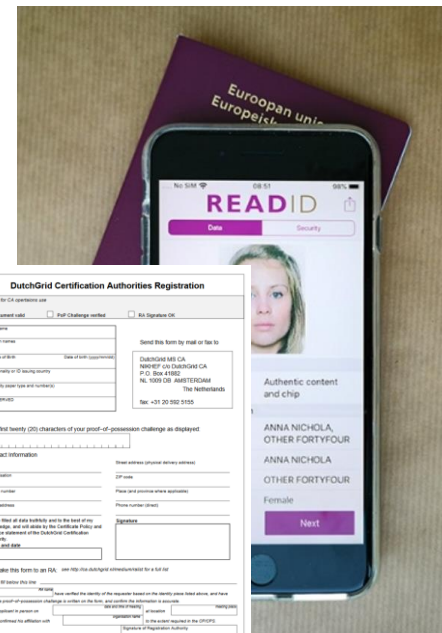
Guest	Subject	Message	Created	Expires	Actions
-------	---------	---------	---------	---------	---------

# Remote identity proofing added

Taking inspiration from HPCI, UK, DigiCert, and AEGON bank, and the hints we already wrote in

<https://wiki.eugridpma.org/Main/VettingModelGuidelines>

- pre-existing business relationship: be in context
- don't call us, we call you ...
- on 'HD' video: show photoID, application form, CSR hash
- do the signing in real-time (not pre-signed)
- prove authenticity of photoID document by live-using the ReadID demo app by Innovalor -- *SURF working on integrated variant for its 'SURFSecureID'*
- signature of the RA replaced by a nonce that the RA will send itself to the CA, to bind the form and the CSR to the meeting



DutchGrid Certification Authorities Registration

Remember to fill out this form on a computer or tablet.

No Document used,  Full Challenge method,  No Signature CA

Given Name: \_\_\_\_\_ Surname: \_\_\_\_\_  
Place of Birth: \_\_\_\_\_ Date of Birth (DD/MM/YYYY): \_\_\_\_\_  
Nationality (or ID country codes): \_\_\_\_\_  
Identify your type and nationality: \_\_\_\_\_  
Nationality: \_\_\_\_\_

Send this form by email or fax to:  
DutchGrid AB CA  
Member of CA CERTIFICOM CA  
P.O. Box 41802  
NL 1009 GB Amsterdam  
The Netherlands  
Tel: +31 20 592 5155

The first twenty (20) characters of your proof-of-possession challenge as displayed: \_\_\_\_\_

Contact Information:  
Name: \_\_\_\_\_ Email address (personal delivery address): \_\_\_\_\_  
Organization: \_\_\_\_\_ Phone: \_\_\_\_\_  
Phone number (personal delivery address): \_\_\_\_\_  
Postal address: \_\_\_\_\_ Phone number (work): \_\_\_\_\_  
I have filled in each field with the best of my knowledge, and will abide by the Certificate Policy and applicable conditions of the DutchGrid Certification Authorities.  
Print and sign: \_\_\_\_\_ Signature: \_\_\_\_\_

Please take this form to an IDV, with the IDV (which is not allowed for a full set ... see our IDV table for the ...  
I have signed the identity of the registrant based on the identity photo taken above, and have had the photo of possession verified in real-time on the live video proofing interface.  
I read the applicant in person on \_\_\_\_\_ (signature) or by video \_\_\_\_\_ (signature) and have confirmed the applicant with \_\_\_\_\_ on the video interface on the IDV/IDP.  
Name: \_\_\_\_\_ Signature of Registration Authority: \_\_\_\_\_

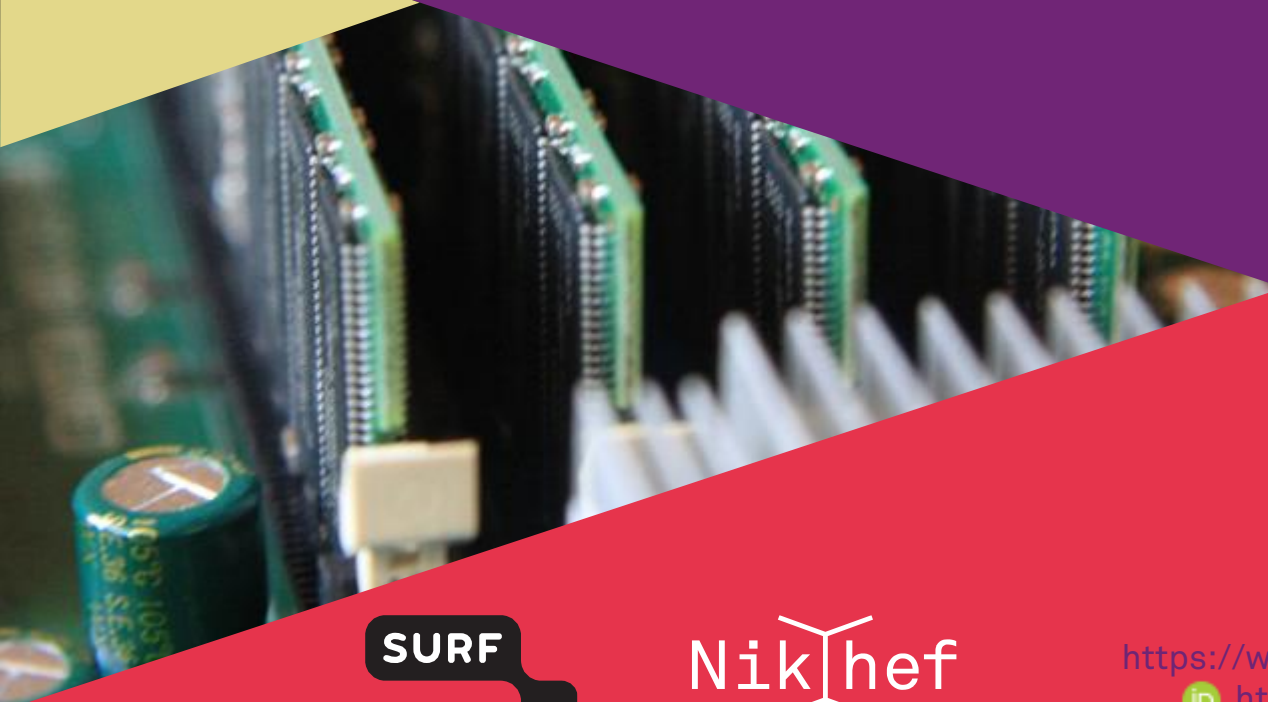
imagery: <https://readid.com> from Innovalor

## CP/CPS update

- circulated CP/CPS update (v3.4) on April 8<sup>th</sup> to the PMA list
- thanks for the comments by Reimer and Dave
- went into effect on April 22<sup>nd</sup>
- in due time, even Nikhef itself may now retire the fax machine (where it may join our “10262 hef nl” Telex endpoint ...)

*luckily, we did not have to use the process yet  
as TCS got a sufficiently-working SAML issuance portal on April 29<sup>th</sup>*





**SURF**

Nikhef

David Groep

davidg@nikhef.nl

<https://www.nikhef.nl/~davidg/presentations/>

 <https://orcid.org/0000-0003-1026-6606>

this work is co-funded by and contributing to the Dutch National e-Infrastructure coordinated by SURF