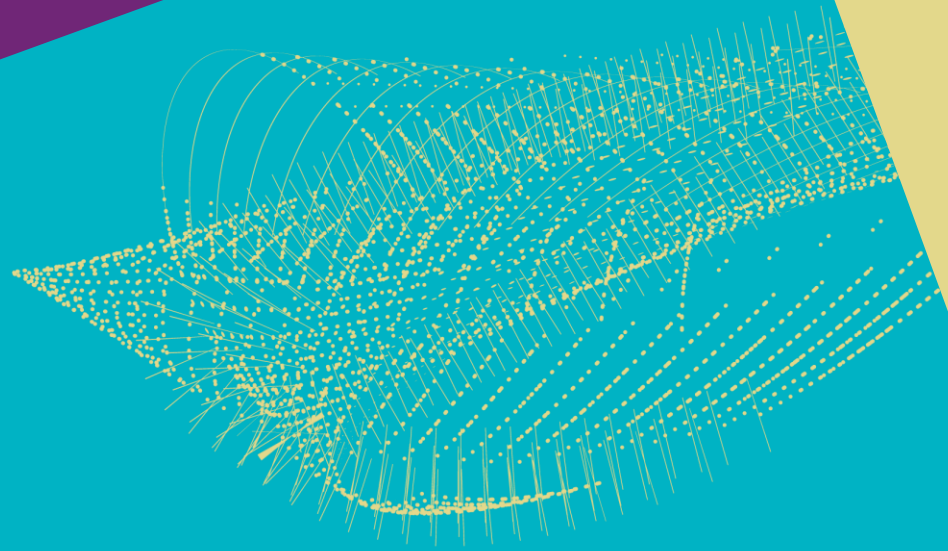
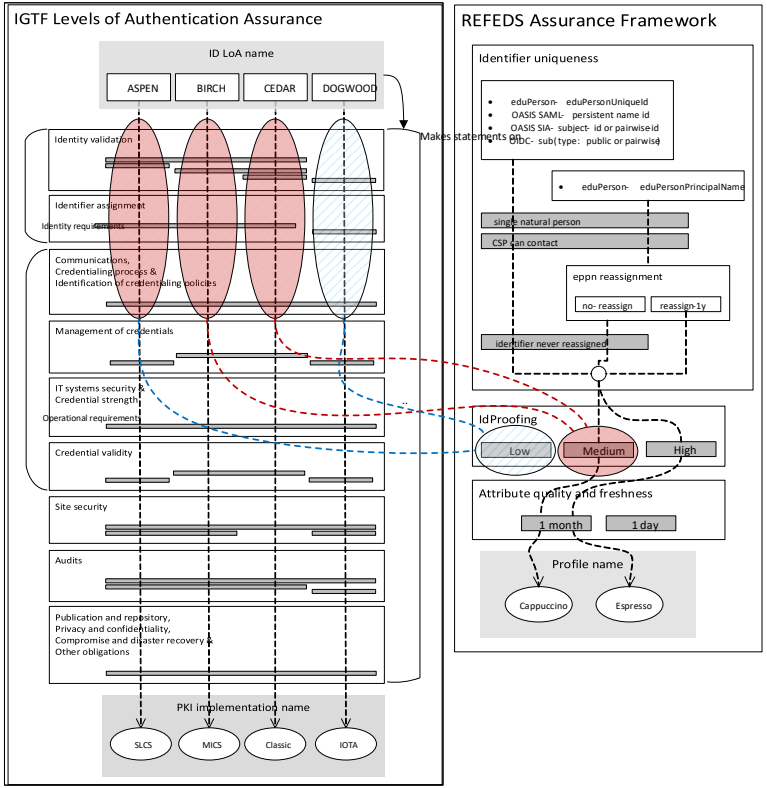
Nikhef



COMBINED ASSURANCE AND THE RPS

THE ‘COMBINED ASSURANCE MODEL’: ID VETTING

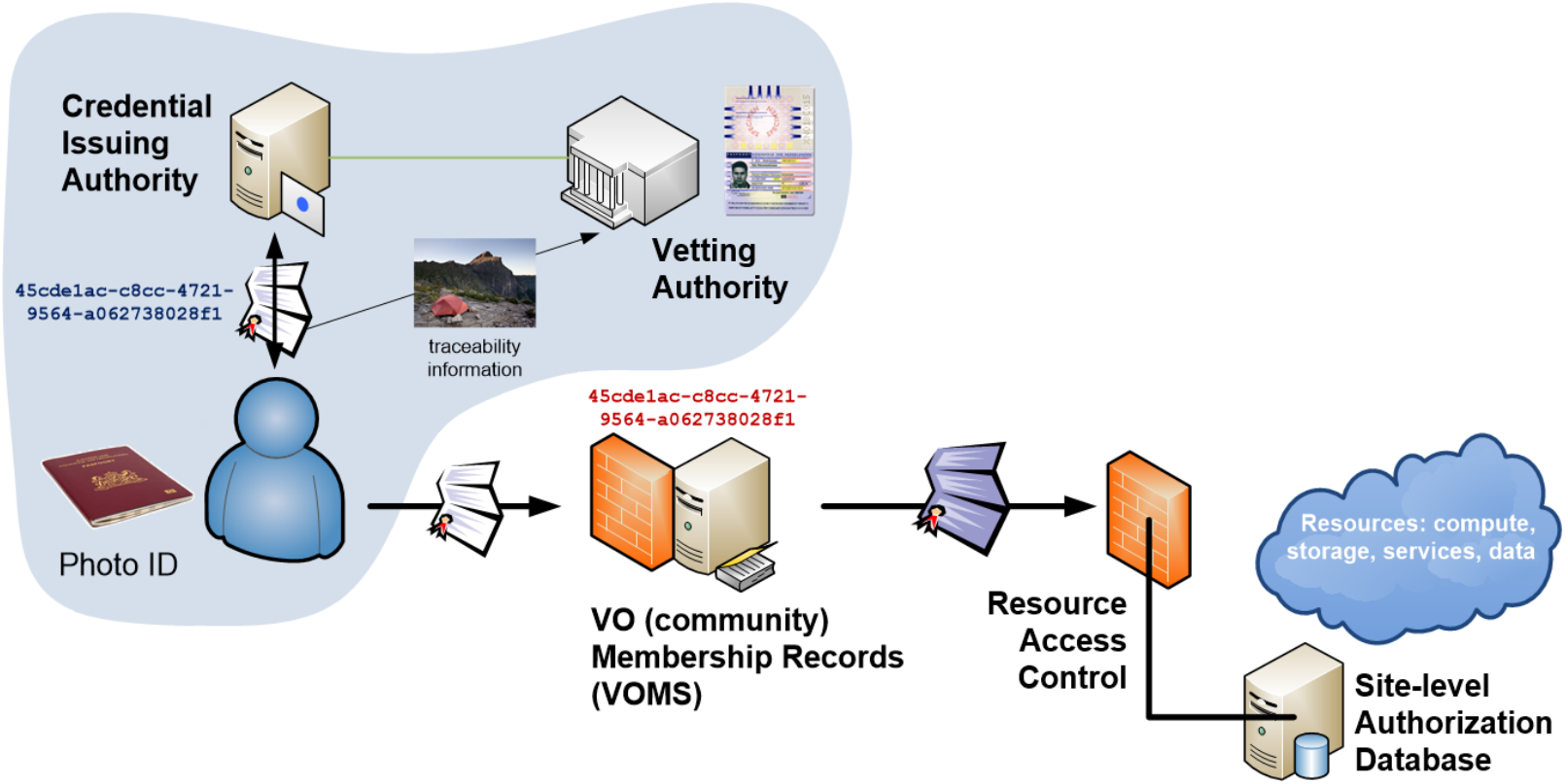


Both IGTF and REFEDS RAF define ‘low assurance’ proofing: basically ‘identifier-only’

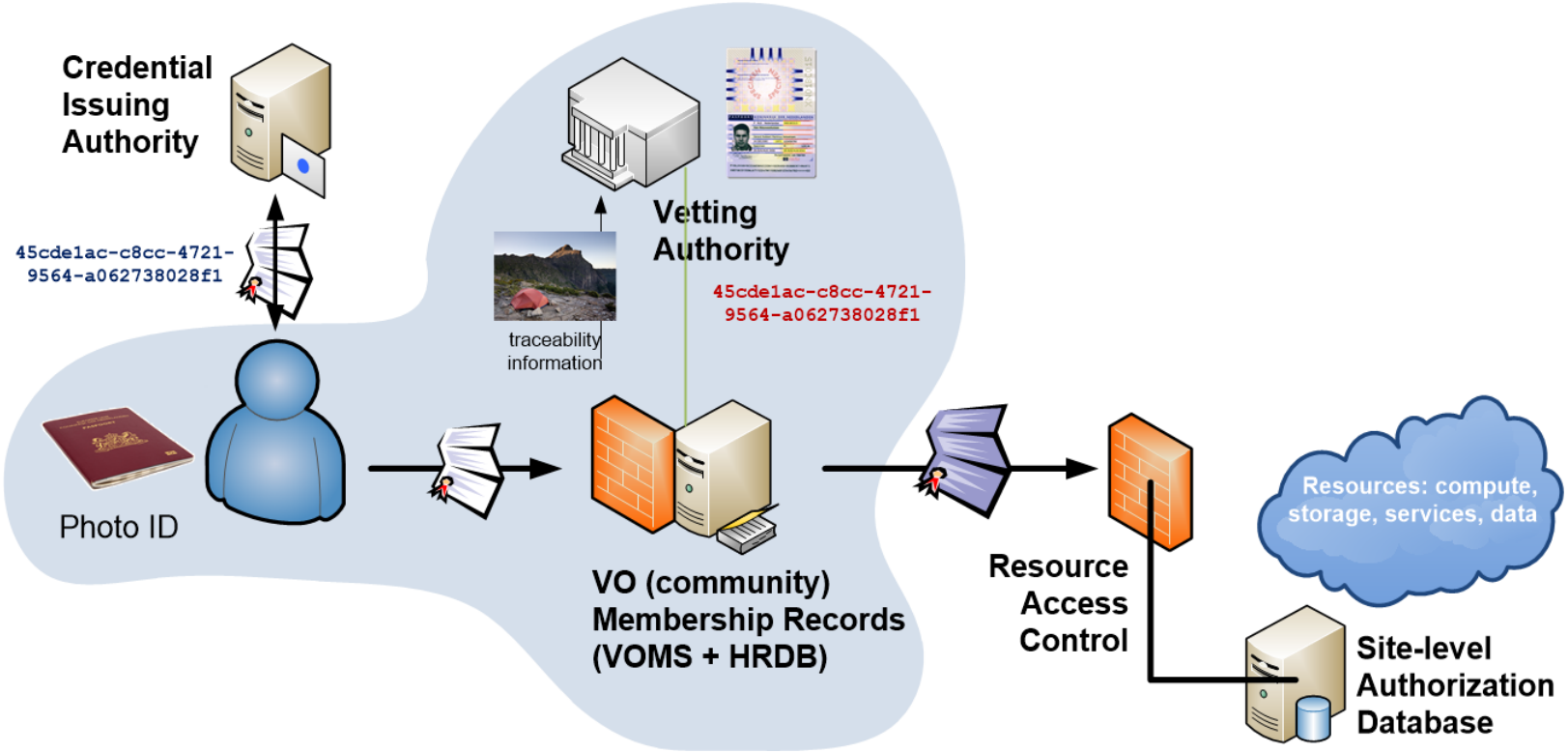
Stepping up to ‘medium’ assurance requires adding a controlled identity vetting process

Who runs that process is selectable!

RESPONSIBILITY MODEL I: TRUSTED THIRD PARTY



RESPONSIBILITY MODEL II: COLLAB. ASSURANCE



SPG ACCEPTABLE AUTHN ASSURANCE

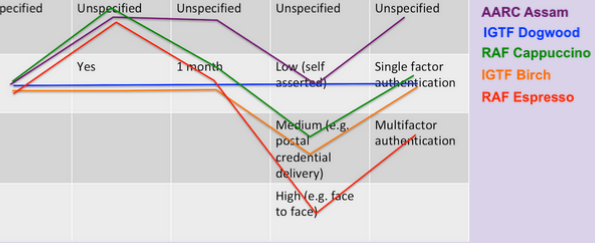
Acceptable Authentication Assurance Policy Template

Questions to ask yourself when defining this policy:

- Which identity providers are acceptable for your infrastructure? SAML Identity Federation IdPs? Social providers such as Google, Facebook etc?
- How much certainty does your community require of the identity? Review each of the elements (personal accounts, uniqueness, freshness, vetting quality, and authentication strength). How will you validate this for each source of (federated) identity?
- How can you ensure that each user is covered by a security incident response capability at their home organisation?
- Do your services, or a subset, require step-up (multi-factor) authentication?

The following chart can be used to help determine an appropriate assurance profile for you. Refer also to AARC Guideline 21:

Should identifiers be unique, personal and traceable?	Should identifiers be unique across the infrastructure?	How fresh do attributes need to be?	What kind of ID Proofing is required?	Is Multi-Factor Authentication required?
Unspecified	Unspecified	Unspecified	Unspecified	Unspecified
Yes	Yes	1 month	Low (self asserted)	Single factor authentication
			Medium (e.g. postal credential delivery)	Multifactor authentication
			High (e.g. face to face)	



Policy Development Kit: Acceptable Authentication Assurance defines the *target level* based on risk assessment

How to *get to the target level* is a process and required procedures

EGI SPG PROCEDURE – ASSESSMENT MATRIX

Policy on Acceptable Authentication Assurance

Document identifier	EGI-SPG-AuthNAssurance-V1
Document Link	https://documents.egi.eu/document/2930
Last Modified	06/01/2017
Version	1
Policy Group Acronym	SPG
Policy Group Name	Security Policy Group

Navigation

- Main page
- Community portal
- Current events
- Recent changes
- Random page
- Help

Toolbox

- What links here
- Related changes
- Upload file
- Special pages
- Permanent link

Page | Discussion

SPG:Drafts:Assessment Community IDvetting adequacy

Authentication and identification is considered adequate, for each User authorised to access Services, if the combined as registration service and/or the Community registration service, meets or exceeds the requirements of the approved IGTF au user credential issuance at their identity provider.

The Community or e-Infrastructure wishing to prove the adequacy of its identity vetting, in order to use its members' credent the Snctfi membership management requirements, must submit a request for assessment by the designated Security Pol

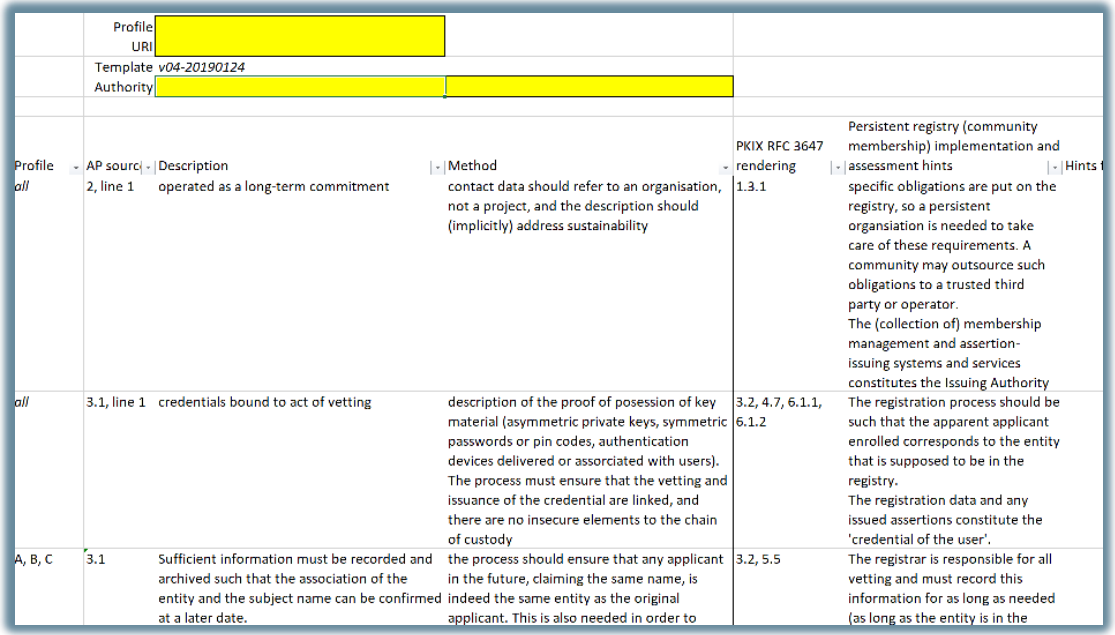
The request shall include the following information:

- a statement of their compliance with the Community Membership Management Policy
- a statement of their compliance with the Community Operations Security Policy
- a documented description of the membership life cycle process and practices meeting the requirements of the IGTF BIR
  - the *credential* of the user is the membership registration data and community-issued assertions
  - the *Issuing Authority* is the collection of membership management and assertion-issuing systems and services
  - the *credential life time* corresponds to the renewal periods as defined in the Community Membership Management P
- a description of the method of binding between the membership information and the DOGWOOD user credential (identif

Based on this information, the SPG shall advise the Infrastructure Operations with respect to suitability of the Community or Authentication Assurance.

The SPG may make available an evaluation matrix. Applicant communities are welcome to use the assurance evaluation *registry (community membership) implementation and assessment hints*. The most relevant community assurance profiles f

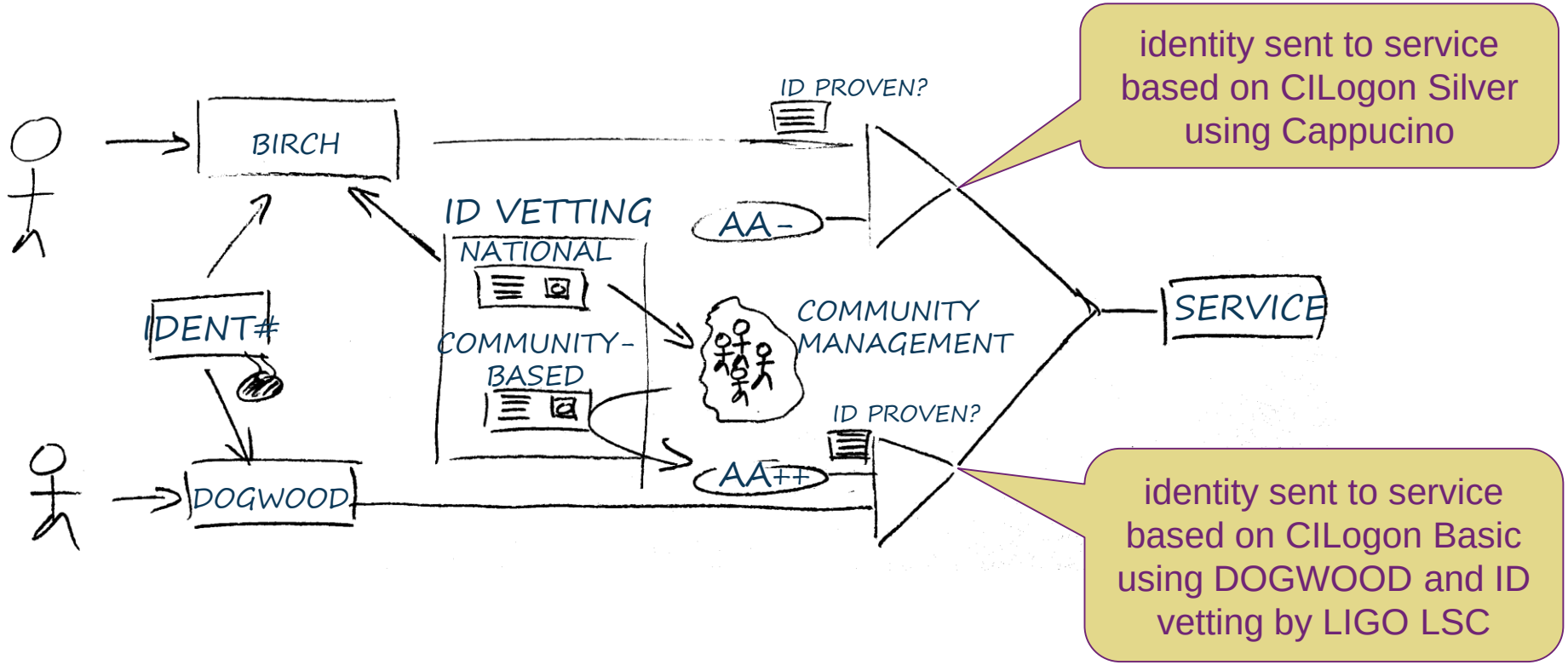
A COMMON ASSESSMENT MODEL ON ID VETTING FOR ID PROVIDERS AND FOR COMMUNITIES



	Profile URI				
	Template	*v04-20190124*			
	Authority				
Profile	AP sourc	Description	Method	PKIX RFC 3647 rendering	Persistent registry (community membership) implementation and assessment hints
all	2, line 1	operated as a long-term commitment	contact data should refer to an organisation, not a project, and the description should (implicitly) address sustainability	1.3.1	specific obligations are put on the registry, so a persistent organsiation is needed to take care of these requirements. A community may outsource such obligations to a trusted third party or operator. The (collection of) membership management and assertion-issuing systems and services constitutes the Issuing Authority
all	3.1, line 1	credentials bound to act of vetting	description of the proof of posession of key material (asymmetric private keys, symmetric passwords or pin codes, authentication devices delivered or assorciated with users). The process must ensure that the vetting and issuance of the credential are linked, and there are no insecure elements to the chain of custody	3.2, 4.7, 6.1.1, 6.1.2	The registration process should be such that the apparent applicant enrolled corresponds to the entity that is supposed to be in the registry. The registration data and any issued assertions constitute the 'credential of the user'.
A, B, C	3.1	Sufficient information must be recorded and archived such that the association of the entity and the subject name can be confirmed at a later date.	the process should ensure that any applicant in the future, claiming the same name, is indeed the same entity as the original applicant. This is also needed in order to	3.2, 5.5	The registrar is responsible for all vetting and must record this information for as long as needed (as long as the entity is in the

https://wiki.eugridpma.org/Main/AssuranceAssessment

BUT THE MODEL EXTENDS BACK TO CAS …



WHAT IS NEEDED IS … THE RPS!

reference RPS targets BIRCH/CEDAR assurance

Scott Rea, in the 33rd EUGridPMA Berlin meeting:

Framework

- "a PKI can establish a set of core documents (with a CP, CPS, subscriber agreement, and relying party agreement) all having the same structure and ordering of topics, thereby facilitating comparisons and mappings among these documents and among the corresponding documents of other PKIs"
- An RPS can be considered as a subordinate document to the CPS

http://wiki.eugridpma.org/Main/RPS

ALIGNMENT AND COMMUNITY GUIDANCE

How to help communities implement community-level ID vetting?

How to engender trust for their service providers?

The ‘increment’ for communities to Cappucino (or IGTF-BIRCH) documented by way of a prefilled RPS as part of the PDK?

Verified using the standard assessment sheet?

What helps the community best?

Nikhef

David Groep
davidg@nikhef.nl
https://www.nikhef.nl/~davidg/presentations/
https://orcid.org/0000-0003-1026-6606