COMMON REQUIREMENT ENUMERATION (CRE)

For successful use and creation of security standards

Rob van der Veer,
representing the team behind opencre.org, including Spyros Gasteratos, Sylvan Rigal and Elie Saad

October 2021

CRE in a nutshell - see opencre.org

- CRE is an **interactive content linking platform** for uniting security standards and guidelines. It offers easy and robust access to relevant information when designing, developing, testing and procuring secure software.
- The idea of CRE is to **link** each small section of a resource to a shared topic identifier(a *Common Requirement*). Through this shared topic link, all resources map to eachother.
- This 1) enables standard and guideline makers to work efficiently, 2) it enables users to find the information they need, and 3) it facilitates a shared understanding in the industry of what cyber security is.
- The key element is **self-maintainability**: the link to CRE from within the standards themselves serves as the input.
- Currently, CRE is **being implemented** as part of the OWASP *integration standards* project.
- Why?
  - **No more difficulty in finding** the right information in the complex landscape of security standards and guidelines
  - **No more broken links**
  - **No more creating and maintaining long mapping tables**
  - **No more having to cover everything in a standard**, just refer to other great resources through CRE
  - **No more silos**

Presenter introduction

Rob van der Veer, representing the CRE initiative with other co-leads: Spyros Gasteratos and Elie Saad

rob.vanderveer@owasp.org

@robvanderveer

+31 6 20437187

- Advisor to ENISA. Co-author of report ‘Advancing software security in the EU’
- Project leader of government-funded research on security requirements
- Project leader at OWASP (Co-lead of the *Integration standards* project)
- Contributor to various standardization initiatives: CIP (Grip on SSD), OWASP (SAMM), NCSC, IEEE, ISO/IEC
- Estabished and leads the security & privacy practice at Software Improvement Group (note: CRE is independent)

Security today is fragmented and complex

ECSO's *Overview of existing Cybersecurity standards* (2018) >200 pages:

Security standards and guidelines: **fragmented, complex and confusing**

For **engineers, testers and procurement**: it's hard to select and find appropriate information in standards

For **standard makers**: it's practically impossible to link to other related work and keep that up to date. Result: standards tend to cover everything, instead of focusing on their added value and link to other work: unnecessary effort and the risk of inconsistencies and incompleteness.

Links to other standards break easily

Some standard

Toegangsvoorzieningsmiddelen inzetten

Richtlijn (wie en wat)
De inzet van identiteit- en toegangsmiddelen levert betrouwbare en effectieve mechanismen voor het vastleggen en vaststellen van de identiteit van gebruikers, het toekennen van de rechten aan gebruikers, het controleerbaar maken van het gebruik van deze middelen en het automatiseren van arbeidsintensieve taken.

Doelstelling (waarom)
Het efficiënter maken van het identiteit- en toegangsbeheer en zorgen dat functies en gegevens uitsluitend beschikbaar worden gesteld aan diegenen waarvoor deze bedoeld zijn als waarborg voor vertrouwelijkheid en integriteit.

Risico
Gegevens worden ingezien, gewijzigd of verwijderd door individuen die hiervoor vanuit organisatie geen toestemming, recht of opdracht hebben.

Classificatie
Hoog

Richtlijn 2012
B0-12, B4-1

Maatregelen

vastleggen van de identiteit

01 Ondersteun de initiële vaststelling en vastlegging van de identiteit van personen met het toegangsvoorzieningsmiddel.
In het toegangsvoorzieningsbeleid is vastgelegd met welke mate van zekerheid de identiteit van een persoon moet worden vastgesteld om deze als gebruiker te mogen registreren.

02 Bied adequate bescherming van de vastgelegde gebruikers- en toegangsgegevens met het toegangsvoorzieningsmiddel.
Wachtwoorden moeten altijd eenwegsvercijferd worden opgeslagen door gebruik van hashing in combinatie met salts.

Het is mogelijk verschillende authenticatiemiddelen te accepteren, die ieder een eigen mate van zekerheid kennen. In dat geval zal bij de autorisatie naar het gebruikte authenticatiemiddel gekeken moeten worden, om te bepalen of de authenticatie voldoende zekerheid geeft om toegang te mogen verschaffen.

04 Ondersteun het wachtwoordbeleid met het authenticatiemiddel.
Voor zover binnen de webapplicatie van wachtwoorden gebruik gemaakt wordt, worden de regels uit het beleid afgedwongen door geprogrammeerde controles.

toekennen van de rechten (autorisatie)

05 Wijs rechten toe op basis van het toegangsvoorzieningsbeleid.

06 Houd een actueel overzicht bij van accounts en de personen die daar gebruik van maken:
- service-accounts;
- beheeraccounts;
- gebruikersaccount;
- (web)applicatie-accounts.

07 Trek de rechten direct in en blokkeer direct het account wanneer een gebruiker geen recht op toegang meer heeft.
Dit gebeurt bijvoorbeeld door uitdiensttreding.

08 Voer periodiek een audit uit op de uitgedeelde autorisaties.

controleerbaar maken van het gebruik

09 Registreer het beheren en onderhouden van identiteiten en autorisatie onweerlegbaar.
Het toegangssysteem en ondersteunde systemen maken gebruik van mechanismen om activiteiten vast te leggen (loggen).

10 Registreer het verkrijgen van autorisatie en het gebruik van functionaliteit onweerlegbaar.

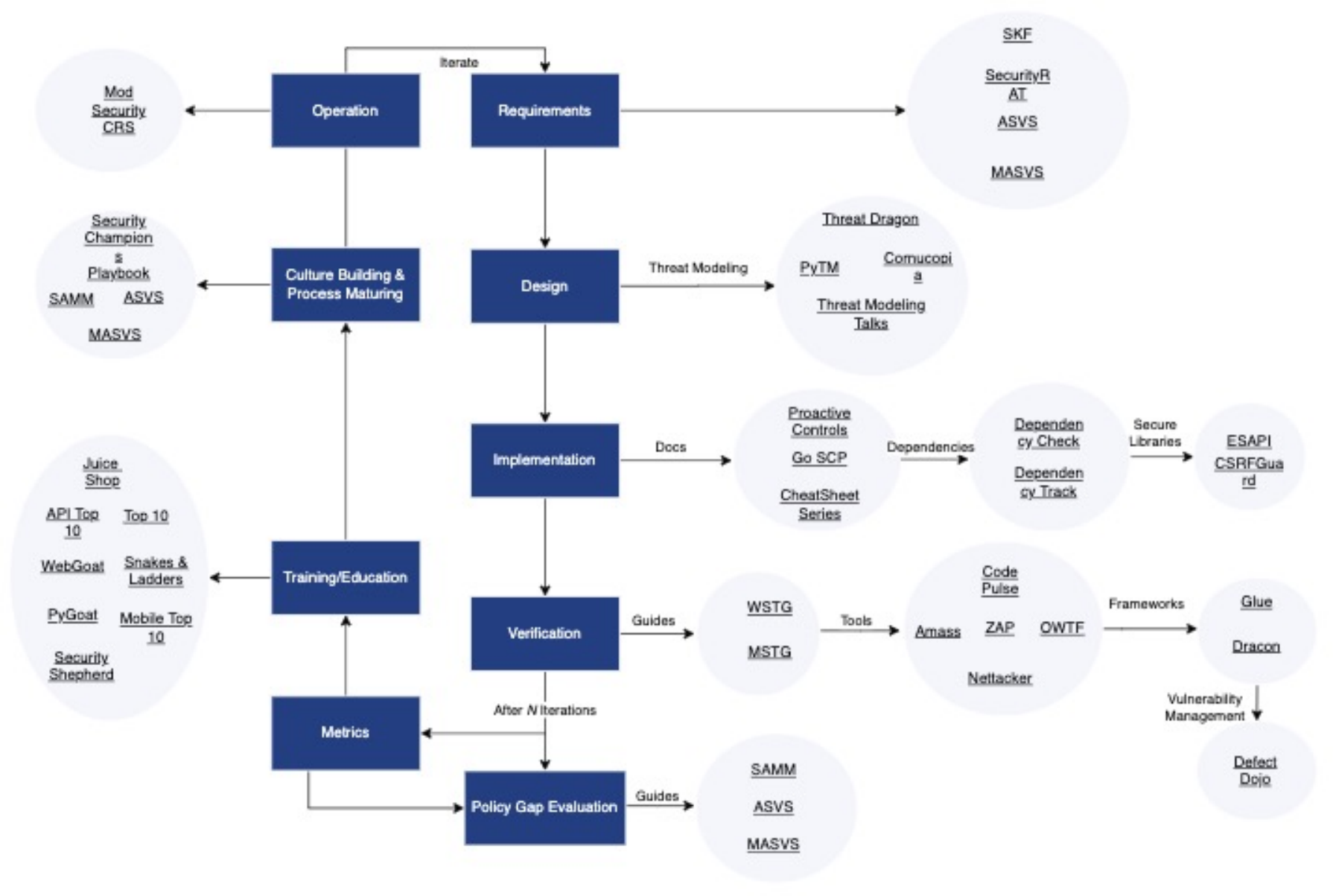
automatiseren van arbeidsintensieve taken

11 Ondersteun met het ingezette identiteits- en toegangsmanagementtool conform het toegangsvoorzieningsbeleid de complete levenscyclus van identiteiten en autorisaties:
- aanvragen;
- toekennen;
- wijzigen;
- intrekken/schorsen/verwijderen;
- conform voorgeschreven procedures.

36 Zie voor afwegingen ten aanzien van de keuze van het authenticatiemiddel: https://www.forumstandaardisatie.nl/fileadmin/os/publicaties/HR_Betrouwbaarheidsniveaus_WEB.pdf

Even OWASP is a puzzle

Application security wayfinder:
https://owasp.org/www-project-integration-standards/



It is time to harmonize security standards

ENISA report:

“Requirements largely overlap, demonstrating that software security is mainly a generic problem and both Standards Developing Organizations (SDOs) and European Standards Organizations (ESOs) or good practice producers are often working without proper coordination and effective liaisons “

“DEVELOP A COMMON REPOSITORY FOR SHARED SECURITY MEASURES”

“Aligning on requirement commonalities across different schemes prevents proliferation and fragmentation, while also making drafting and maintaining a scheme more efficient in terms of mitigating the risks."

Let’s solve this!

Security standards and guidelines are connected at the requirement level

OWASP ASVS 4.02

#	Description
6.1.1	Verify that regulated private data is stored encrypted while at rest, such as Personally Identifiable Information (PII), sensitive personal information, or data assessed likely to be subject to EU's GDPR.

More info on encryption

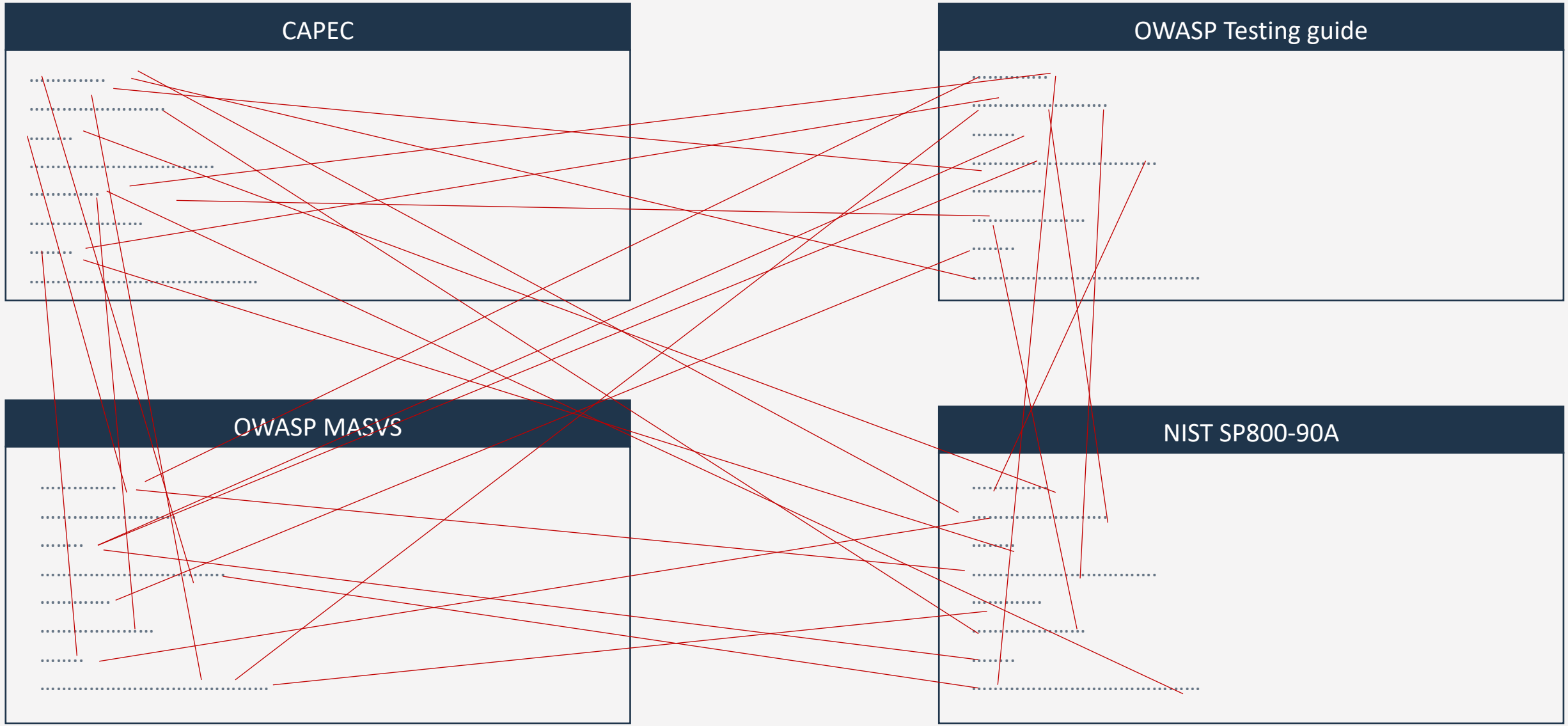
NIST SP800-53 rev.5, SC-12

More info on how to test this

OWASP Web Service Testing Guide 4.0, CRYP-04

If we could connect everything, things would become easier, clearer, more consistent, more complete. But how?

Problem 1:
Mapping everything to everything is too much work and unmaintainable

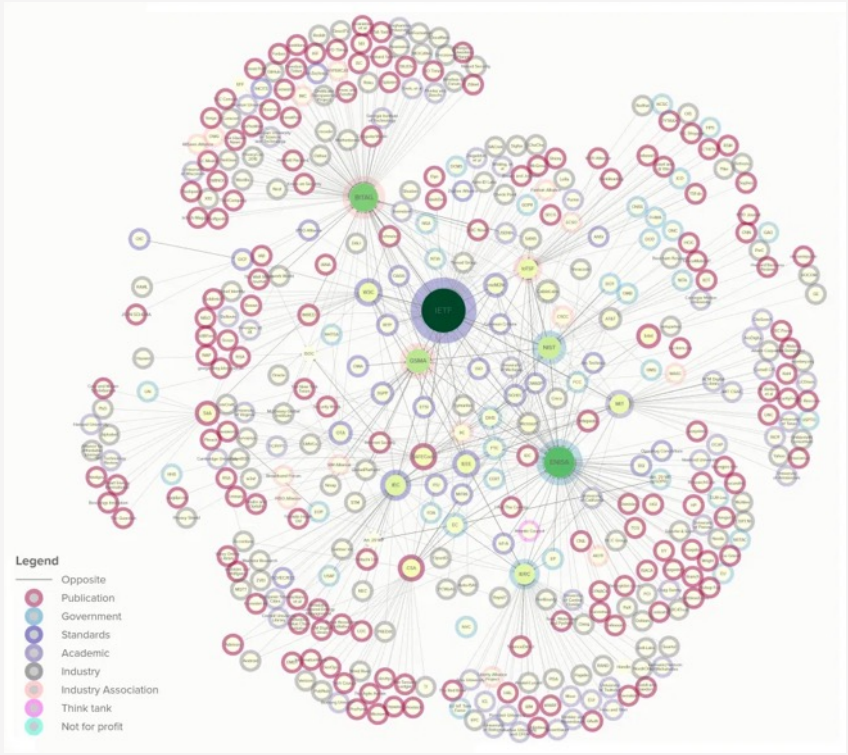


Example of problem 1: iotsecuritymapping.uk

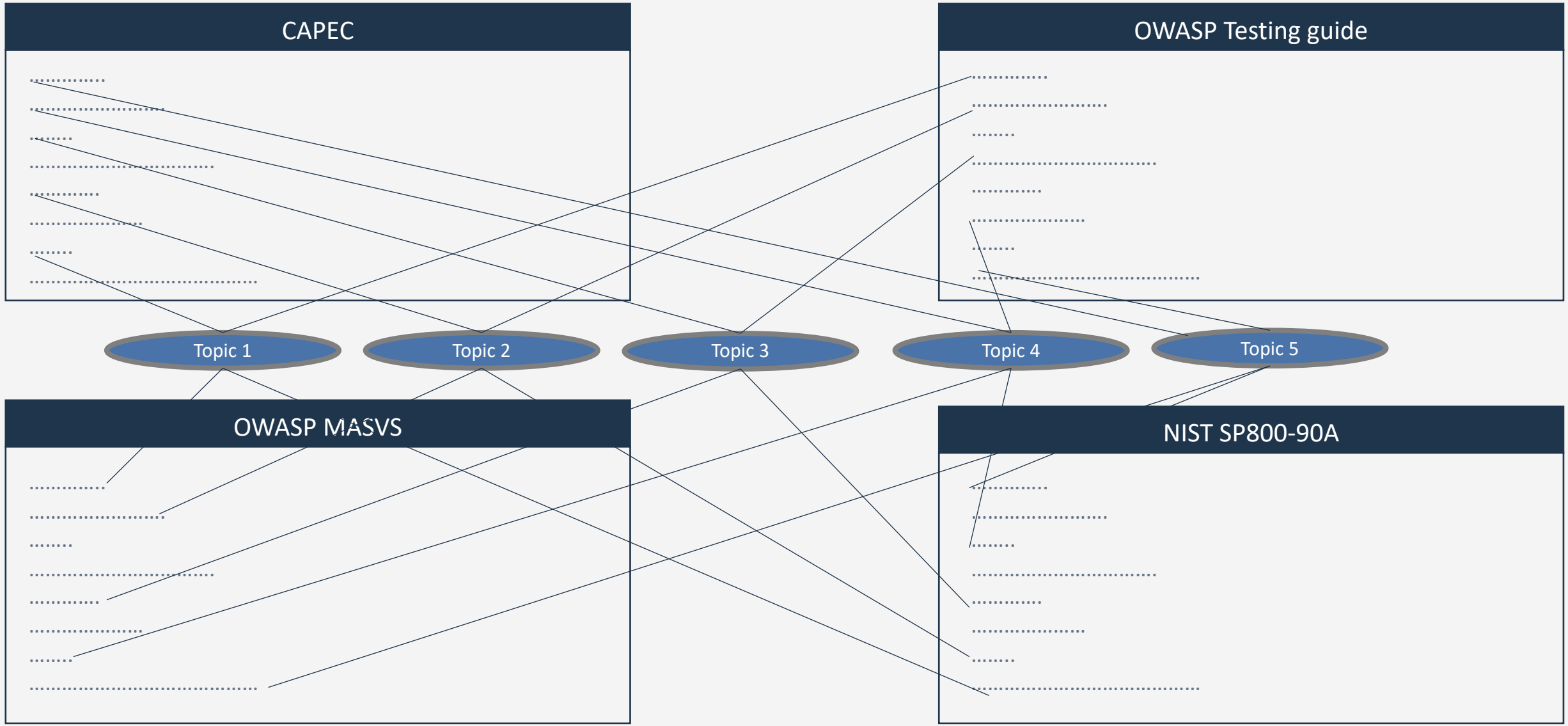
Iotsecuritymapping.uk mapped IoT security standards, from a hundred sources.

Result: a thousand pages of JSON specifications. A useful effort but **extremely hard to maintain**

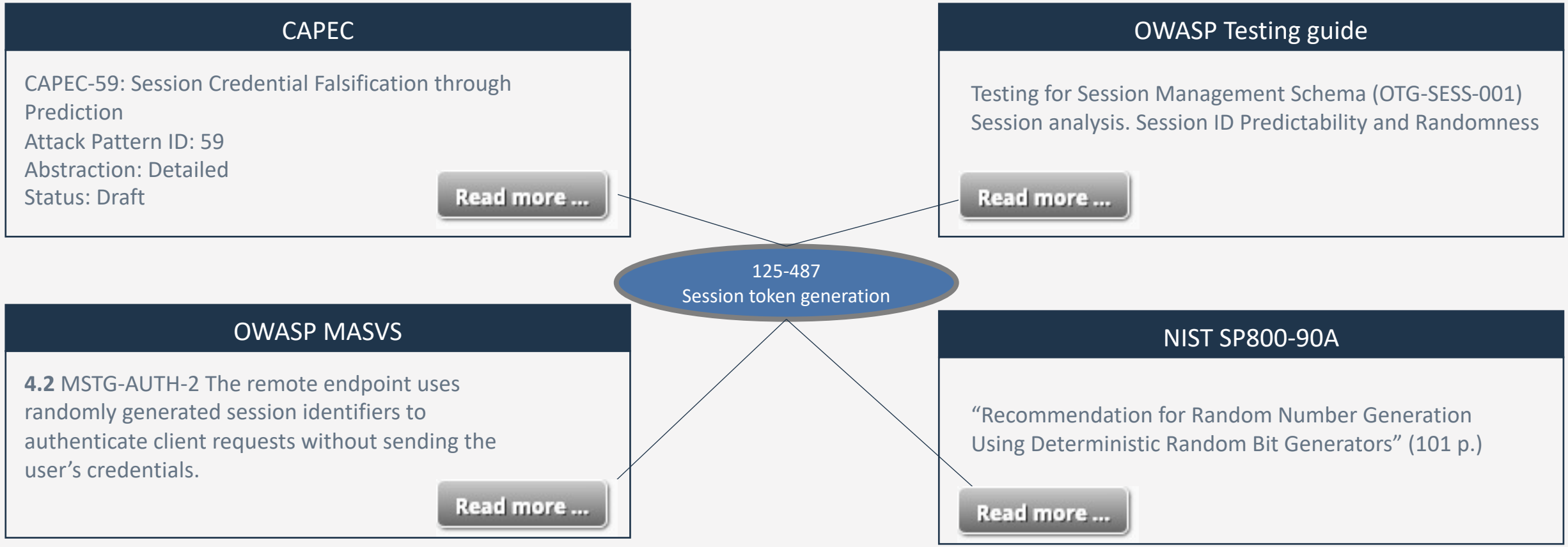
Imagine doing this for all security topics.



Solution 1: only link to one set of shared topics, not to all other standards

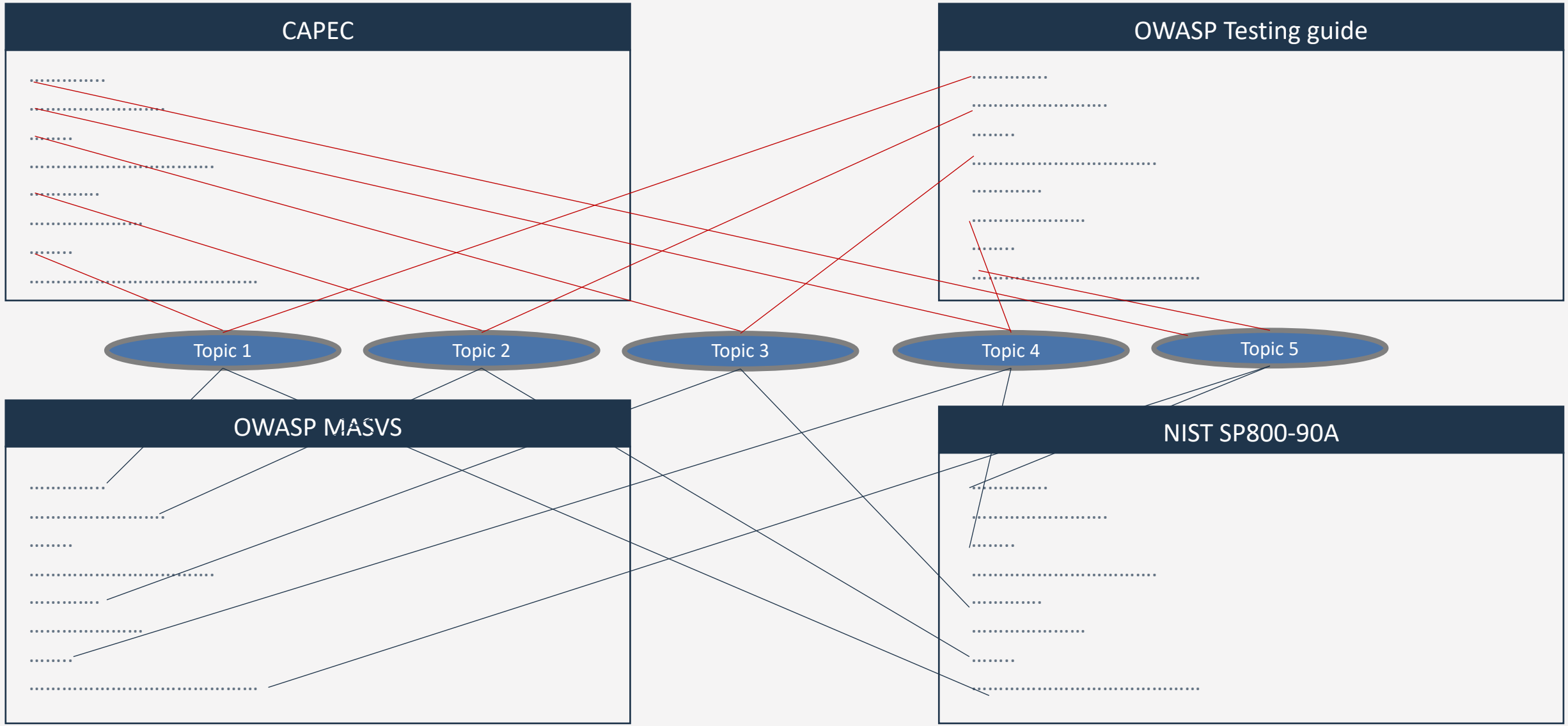


Example of linking to a shared topic

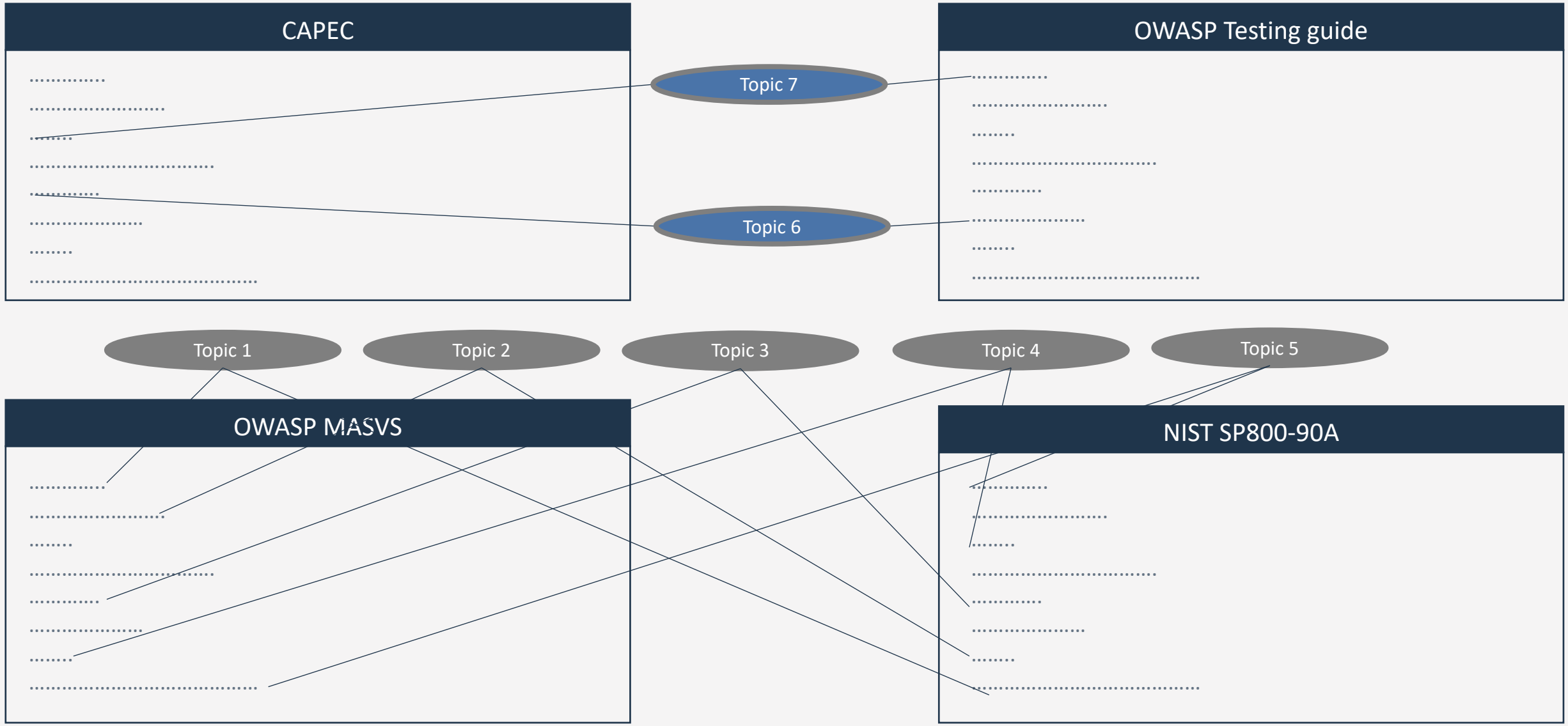


Each section in a standard links to the corresponding Common Requirement and by doing so, standard sections link to each other. This allows readers to find all the information they need on a topic, as if they were using one single source – without links becoming outdated.

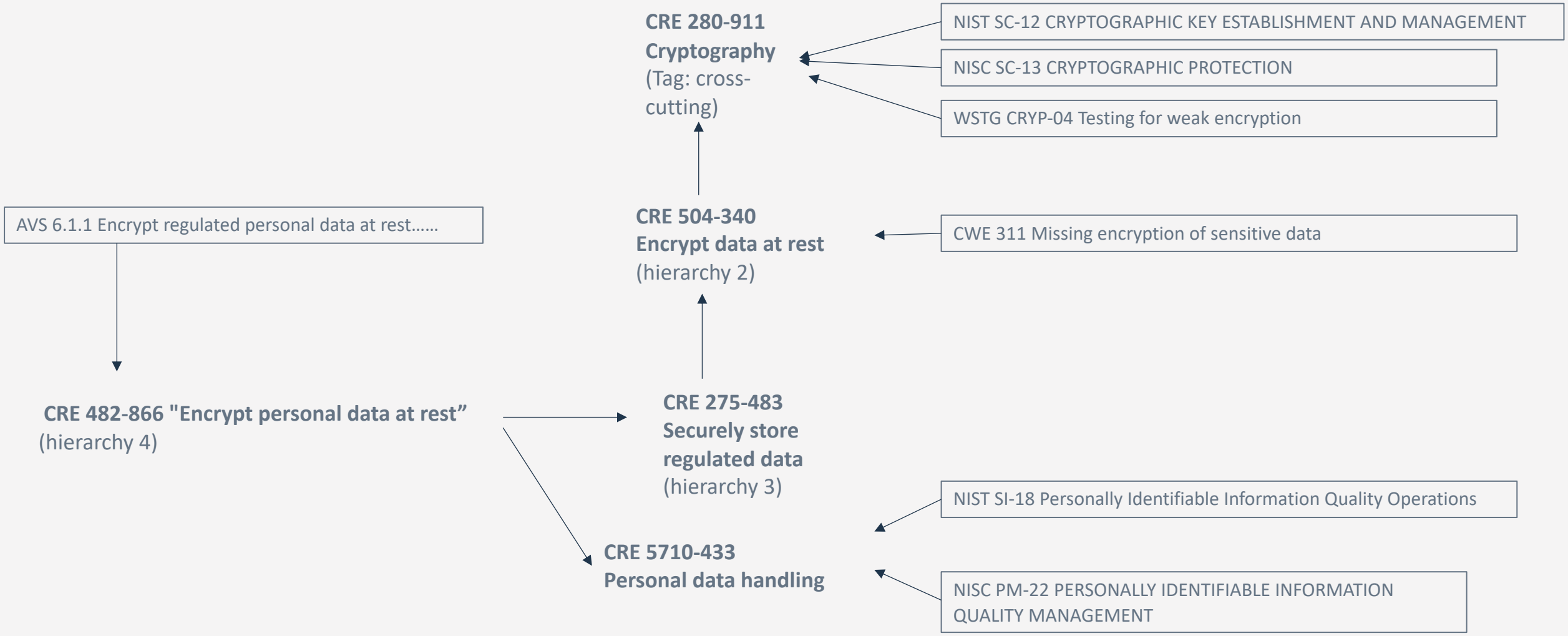
Problem 2: as a standard, finding the right CRE topics is much work



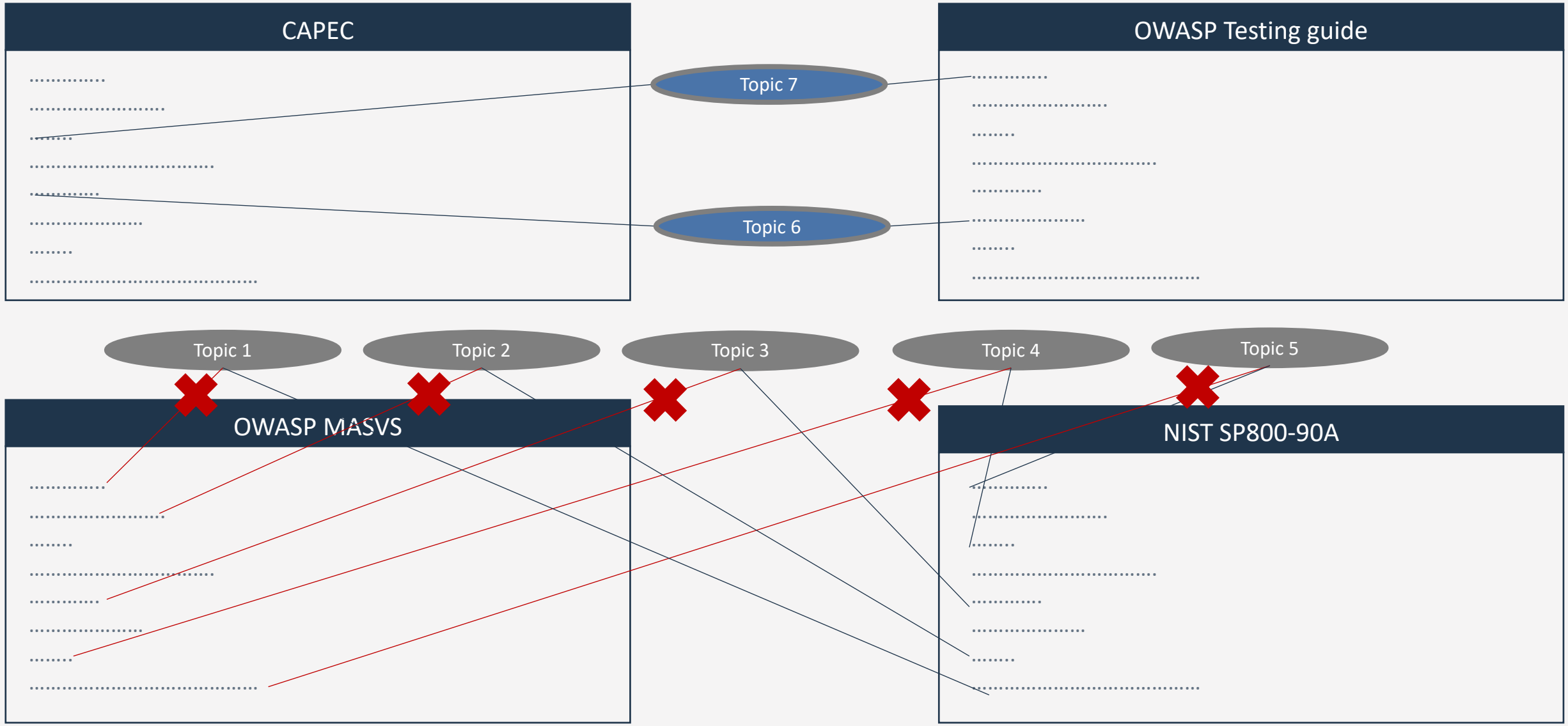
Solution 2: introducing higher level topics: easier linking



Example of higher level topics: easier linking, and as a bonus: structure



Problem 3: standards change and links break



Solution 3: the link to the topic in the standard IS the mapping

CAPEC

CAPEC-59: Session Credential Falsification through Prediction
Attack Pattern ID: 59
Abstraction: Detailed
Status: Draft

125-487

OWASP Testing guide

Testing for Session Management Schema (OTG-SESS-001)
Session analysis. Session ID Predictability and Randomness

125-487

OWASP MASVS

4.2 MSTG-AUTH-2 If stateful session management is used, the remote endpoint uses randomly generated session identifiers to authenticate client requests with[illegible]dentials.

125-487

NIST SP800-90A

“Recommendation for Random Number Generation Using Deterministic Random Bit Generators” (101 p.)

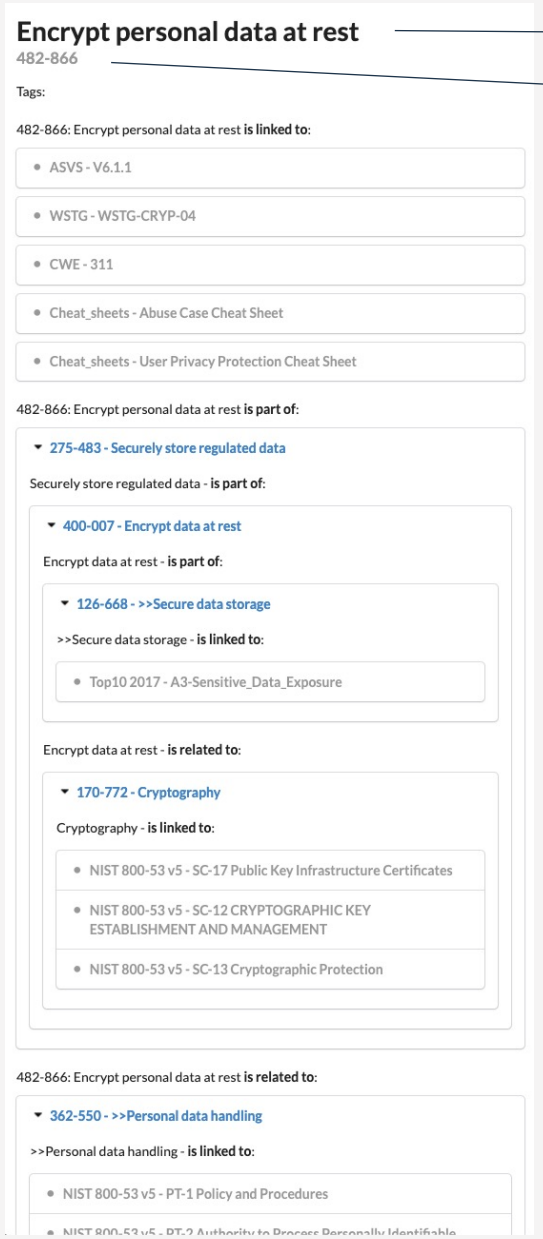
125-487

Because the link to the CRE topic is IN the standards, the ID can be parsed and the mapping becomes self-maintaining.

Enter the CRE. What did we do?

1. After extensive research and interviews with standard makers, procurement, industry, academia, engineers, testers and certification bodies, **the idea for CRE was born**.
2. Assembled a **group of people** - “Integration standards” project at OWASP
3. **Workshops** with standard makers and security professionals to understand issues
4. Designed **linking mechanism**
5. Created **mapping**: ASVS, Top10, NIST 63, NIST 53, OCP, Cheat sheets, WSTG, CWE (kudos ASVS and SKF teams)
6. Created the **CRE topic tree**: emerged as consensus from these standards, plus the SIG ISO25010 security model.
7. Worked with **stakeholders**: OSSF, Top 10 team, CIP, etc.
8. We built the CRE application: **opencre.org**. Everything is open source.

Example of a page on opencre.org



The Common requirement ‘Encrypt personal data at rest’

Its unique code

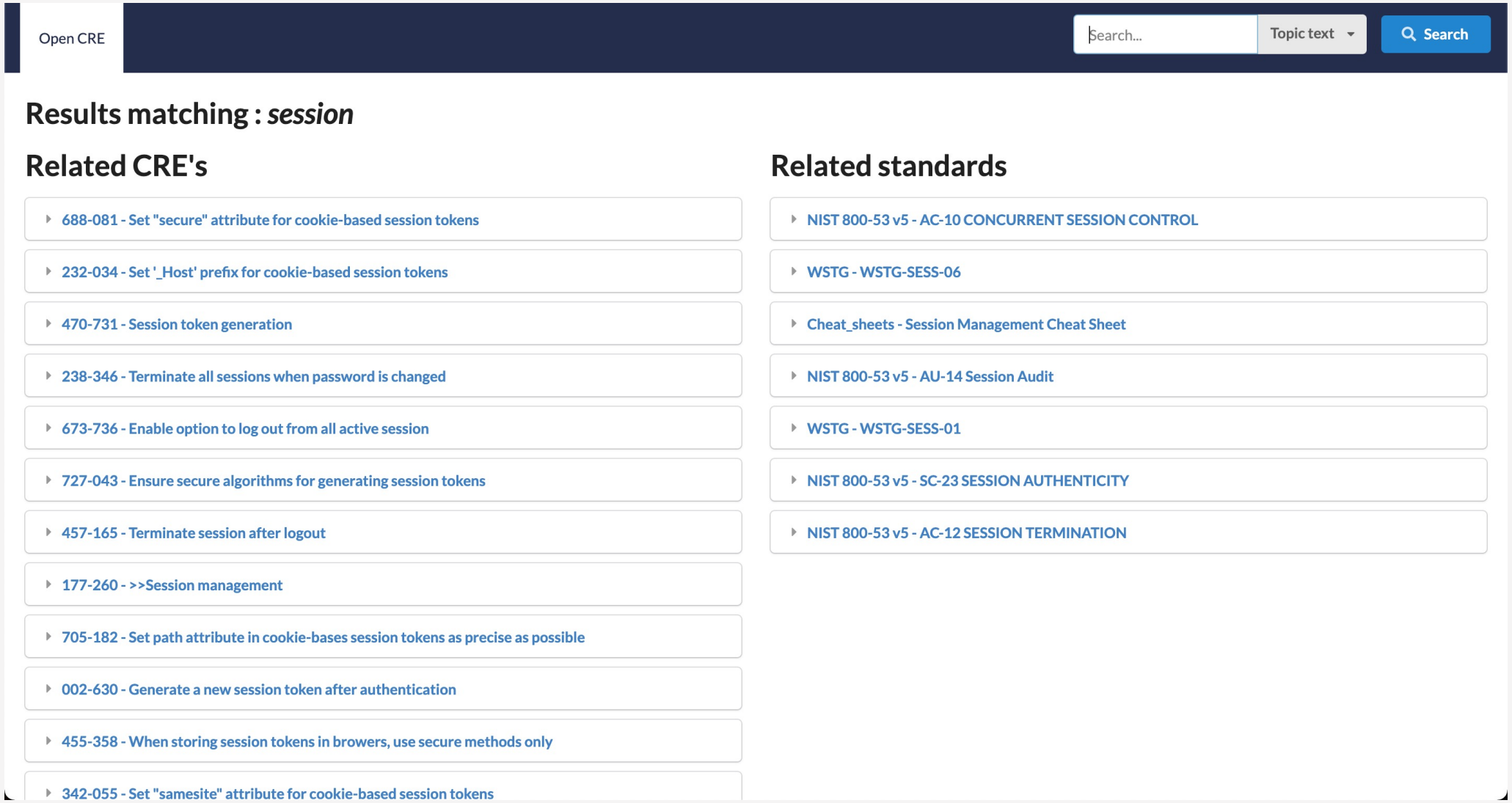
Standard entries linked to this requirement, all clickable

Higher level topics, that are again linked (eg. Owasp top 10) and by clicking on them the user can explore these topics, subtopics and related topics

Related topic *Cryptography*, again with links to standards

Related topic *personal data handling*

Example of a search on opencre.org



How does the self-maintenance work?

CRE supports two models of maintaining links:

1. A **mapping file** for a standard that contains the CRE identifiers that are covered with the hyperlinks to where they are covered. This can be maintained by a third party (e.g. the CRE team) and ideally by the standard maker.
2. **Embedded mapping**: the source files of the standard contain the CRE links which are scanned by the CRE parser to automatically create the mapping file. This approach makes things completely self-maintaining.

Example:

OWASP MASVS
** 4.2MSTG-AUTH-2 ** If stateful session management is used, the remote endpoint uses randomly generated session identifiers to authenticate client requests without sending the user's credentials. Read more

The CRE parser is configured to scan for CRE references (last line) and then register the CRE identifier and link that to the first section before that link with the class "ruletitle" and pick the corresponding ID (first line).

In this example this leads to the following entry in the mapping file:

125-487, http://www.owaspmasvs.org/rules.html#rule123

More advanced features in the making

Reference flexibility:

- Using the CRE mechanism it is also possible to **deeplink directly** to a specific source, which is automatically kept up to date.
- Similarly the CRE **URL can control how** the information is presented (e.g. OWASP sources first)

Furthermore, **users can manage** their own account or sessions on the CRE website and specify what sources they prefer to see.

Data analysis: The (anonymous) use of CRE leads to interesting insights into the use of standards and specific topics.

Search: while parsing all source files, an index may be built to allow 'federated' search over all sources.

Map/gap analysis: using CRE it is easy to map standard X to standard Y to verify compliance across standards, and also to find gaps.

Summary

The CRE enables **alignment and cross-reference** between security standards and guidelines, to:

- Make it easier for **standard makers**
- Make it easier to **find and use** relevant information for engineers, testers, auditers and procurement

Bonus:

- Attain **shared understanding** in market and industry on what security means
- Achieve **more consistency and less gaps** between standards

The future is simple

Call to action

Use www.opencre.org and spread the word (e.g. social media)

Provide your feedback and ideas: https://github.com/OWASP/common-requirement-enumeration/

Contribute: https://github.com/OWASP/common-requirement-enumeration/blob/main/CONTRIBUTING.md

Also: share mappings if you have them

Join the mailing list: project-cre@owasp.org

Join our team: https://owasp.org/www-project-integration-standards/

Standard makers unite! And start using the CRE:

- Links to other standards wil never break
- Your standard becomes instantly accessable through CRE
- Provide your viewers access to a large range of related resources, so you won't need to discuss all these topics yourself
- Join our stakeholder group to help steer the CRE direction