Using openCRE.org to master application security

Spyros Gasteratos

May 2022

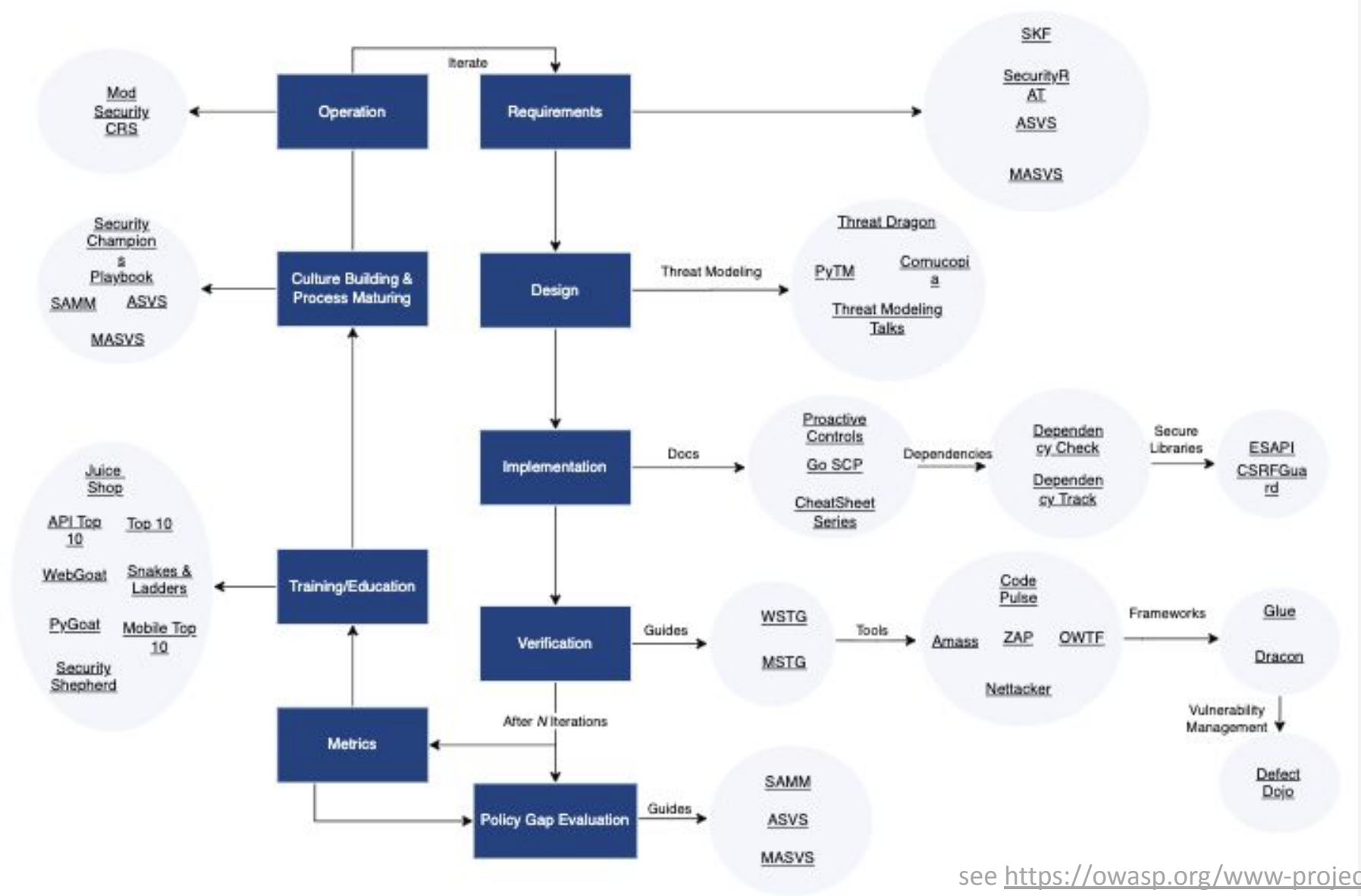
Presenter introduction

Spyros Gasteratos

@0xfde

- Application Security Lead @Thought Machine – Hiring!
- Co-lead of THE OWASP *Integration standards* project
- Open Source Developer (Dracon, SKF etc)
- OWASP volunteer

We built *Security wayfinder*, because finding info at OWASP can be a struggle



see https://owasp.org/www-project-integration-standards/

The problem: finding relevant security info today is a struggle in general

Overview of existing Cybersecurity standards* **>200 pages:**

The security standards and guidelines landscape is **bulky**, **fragmented, complex and confusing**

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

For **standard authors**: it's practically impossible to link to other related work and keep that up to date.

(*) ECSO 2018

It is time to create a unified repository of security requirements

ENISA report:

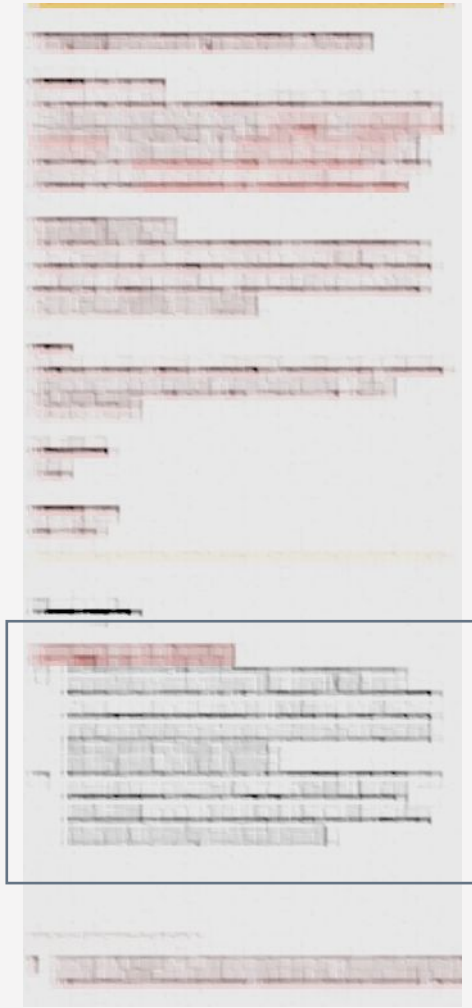
“Requirements largely overlap, demonstrating that software security is mainly a generic problem and both Standards Developing Organizations (SDOs) and European Standards Organizations (ESOs) or good practice producers are often working without proper coordination and effective liaisons “

“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."

Example of the struggle: trying to cover a topic in a national standard

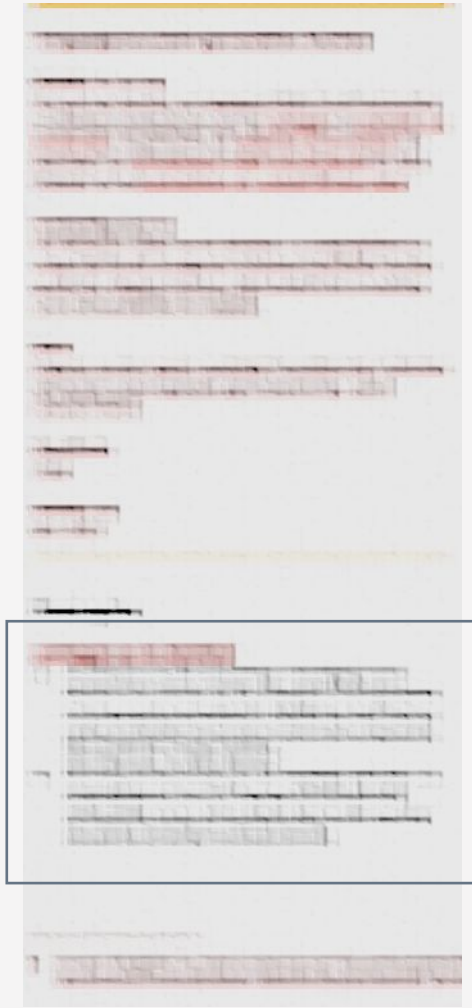
Secret management



References:
-OWASP Top 10 Sensitive data exposure
-CWE 123
-CWE 456
-Pro active controls C6
-X
-Y
-Z

Example of the struggle: trying to cover a topic in a national standard

Secret management



References:
-OWASP Top 10 Sensitive data exposure
-CWE 123
-CWE 456
-Pro active controls C6
-X
-Y
-Z

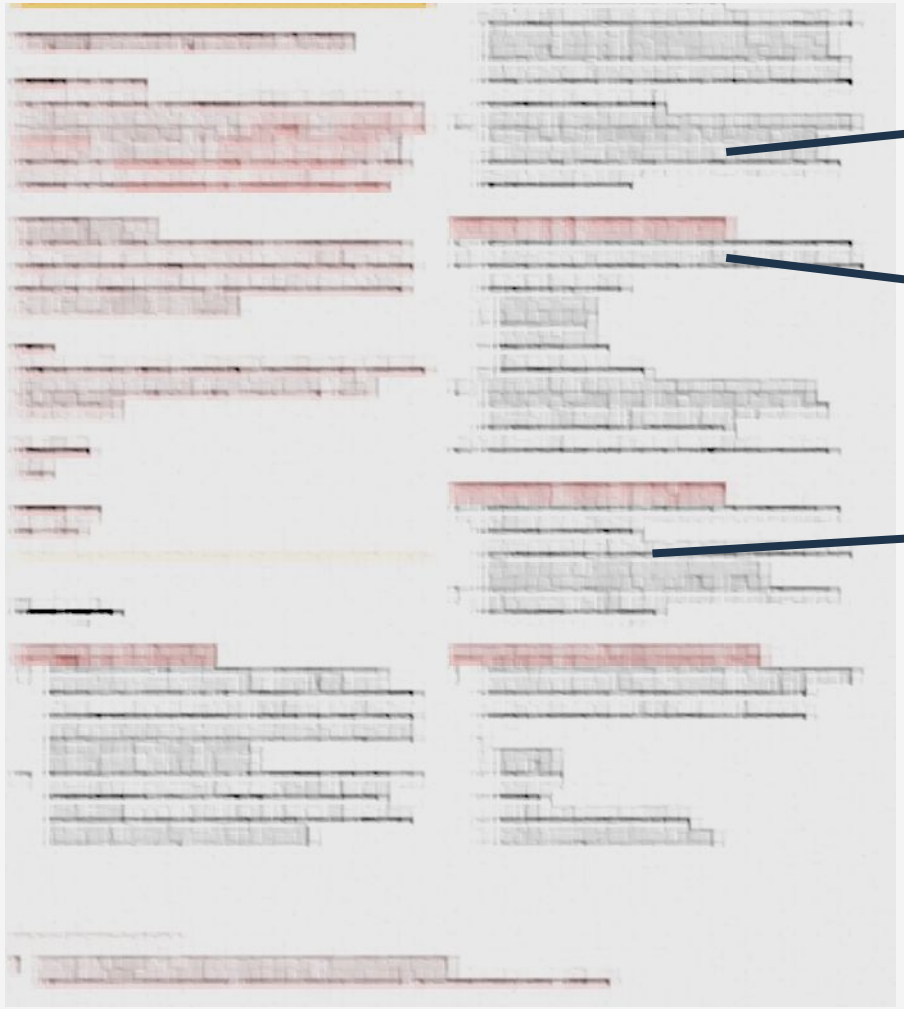
No structure, unclear why referred

Old version

Great resources missing

Example of the struggle: trying to cover a topic in a national standard

Secret management



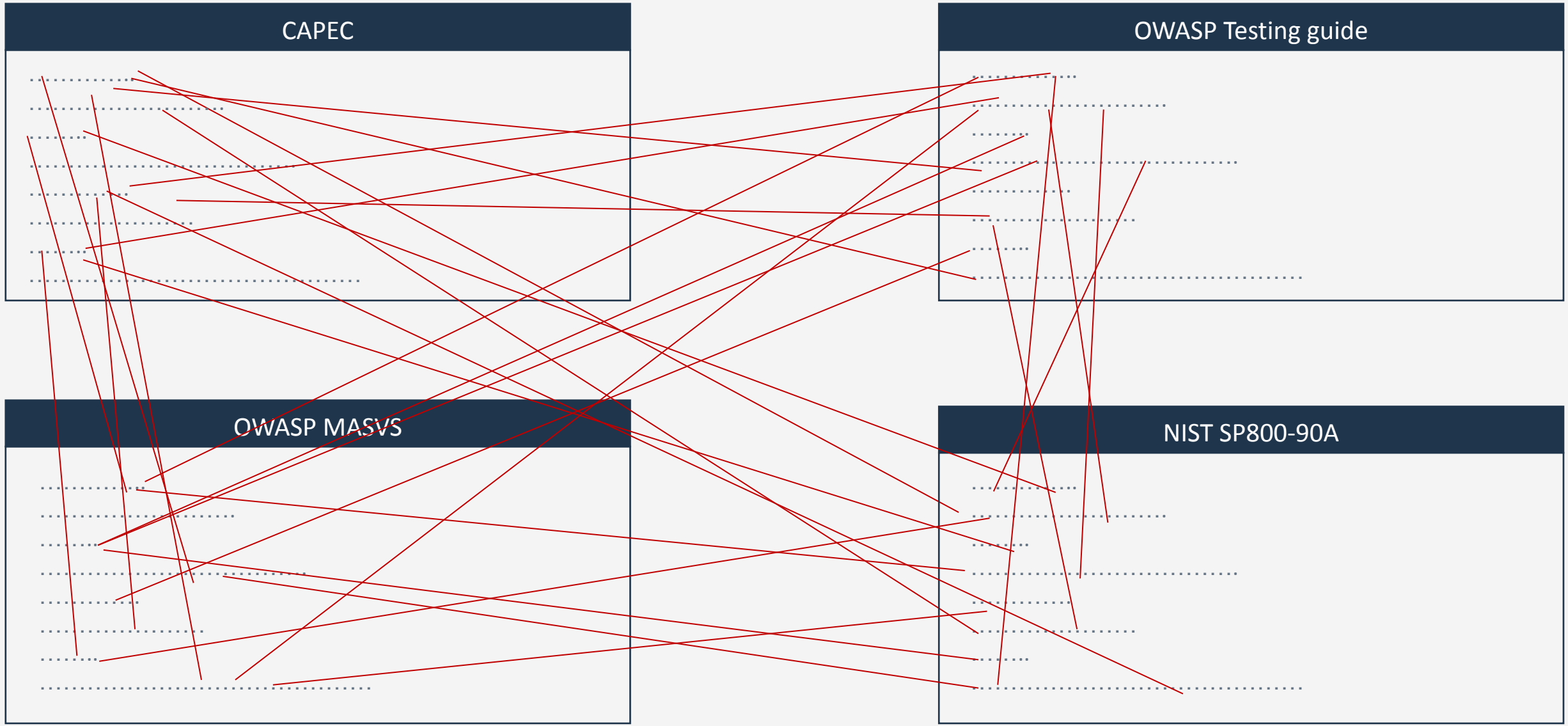
Not the expertise of the author. Inconsistencies

Quickly outdated

Incomplete

More bulk, more fragmentation

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

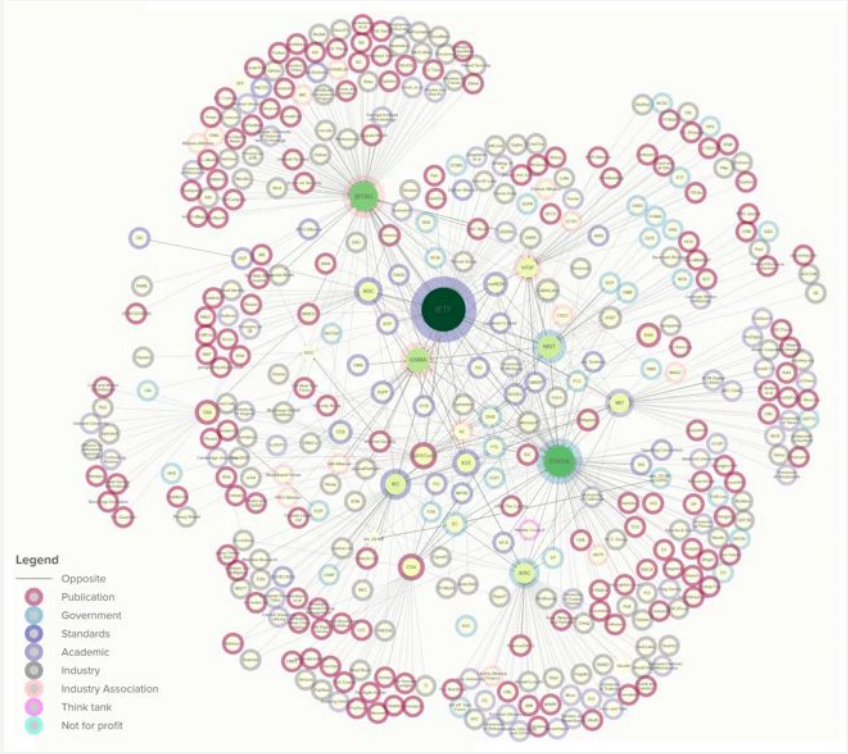


Example of problem 1: iotsecuritymapping.uk

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.



Connecting standards 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

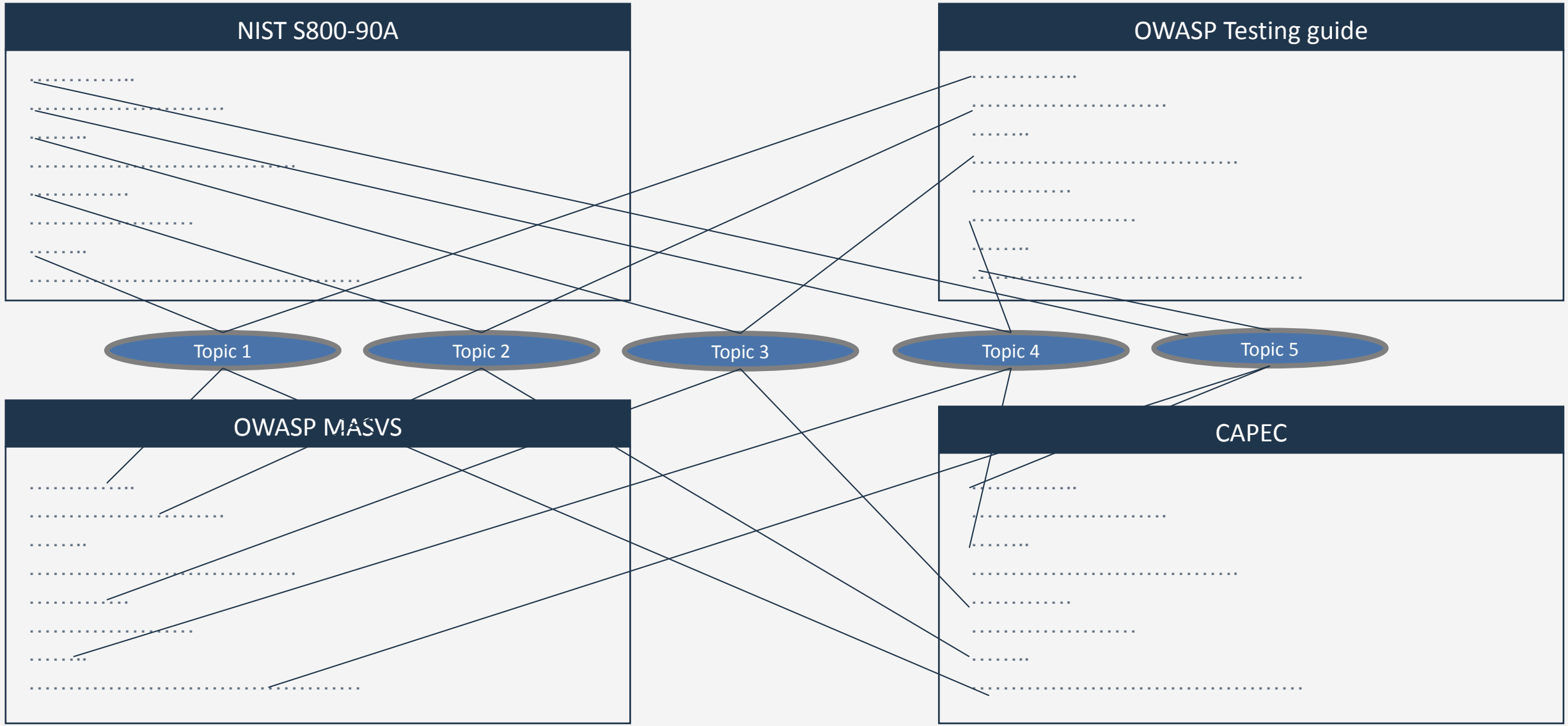
NIST SP800-53 rev.5, SC-12

More info on how to test this

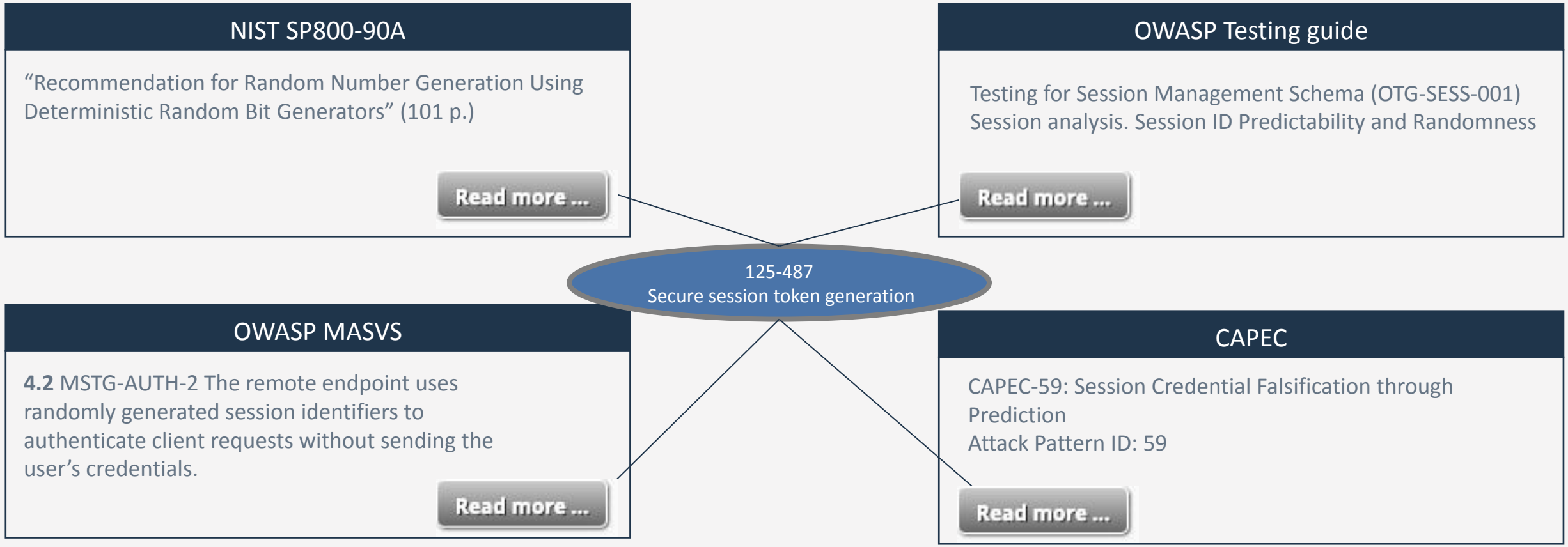
OWASP Web Service Testing Guide 4.0, CRYP-04

How could we link everything together, AND keep it up to date ??

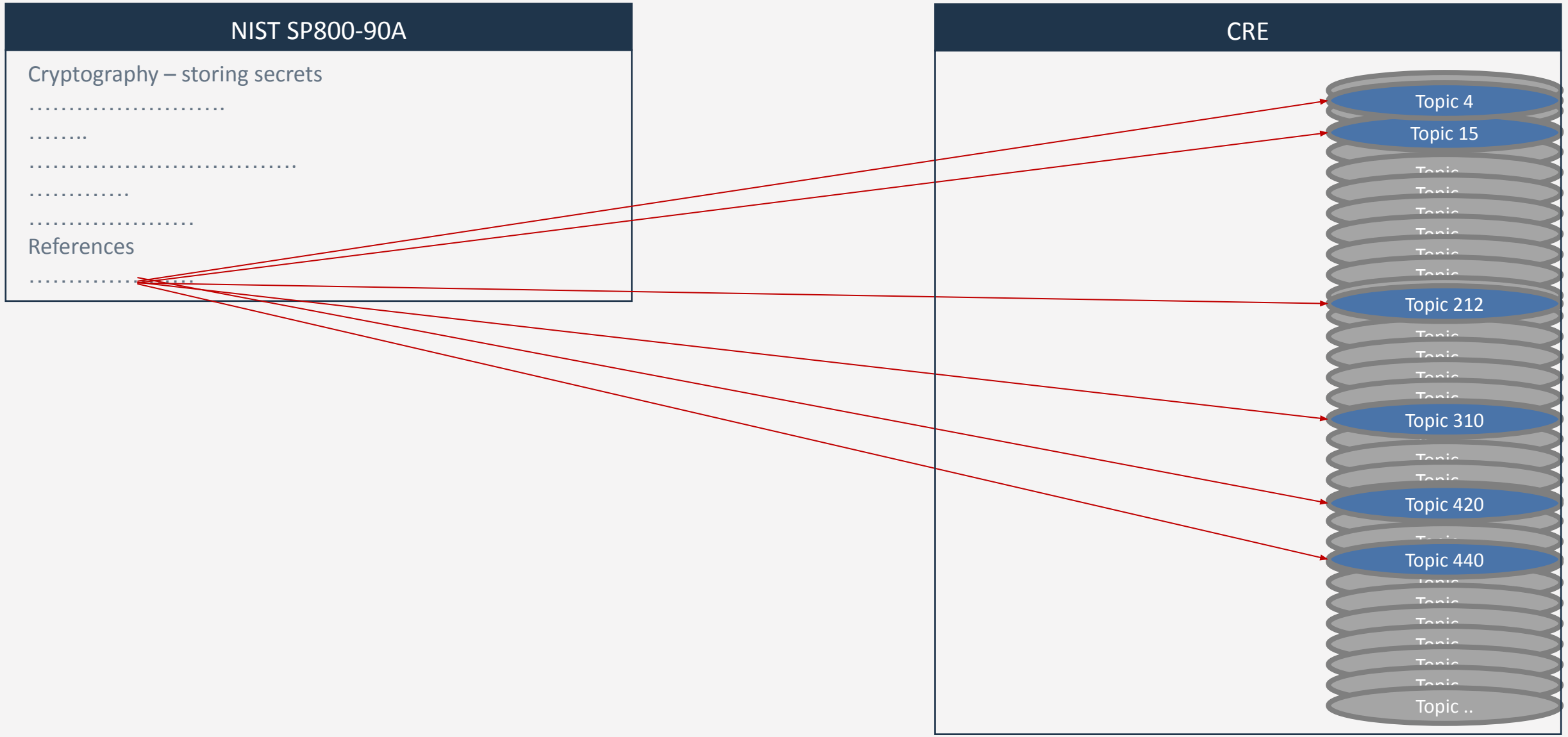
Solution 1: don't link directly between standards. Link to a set of shared topics



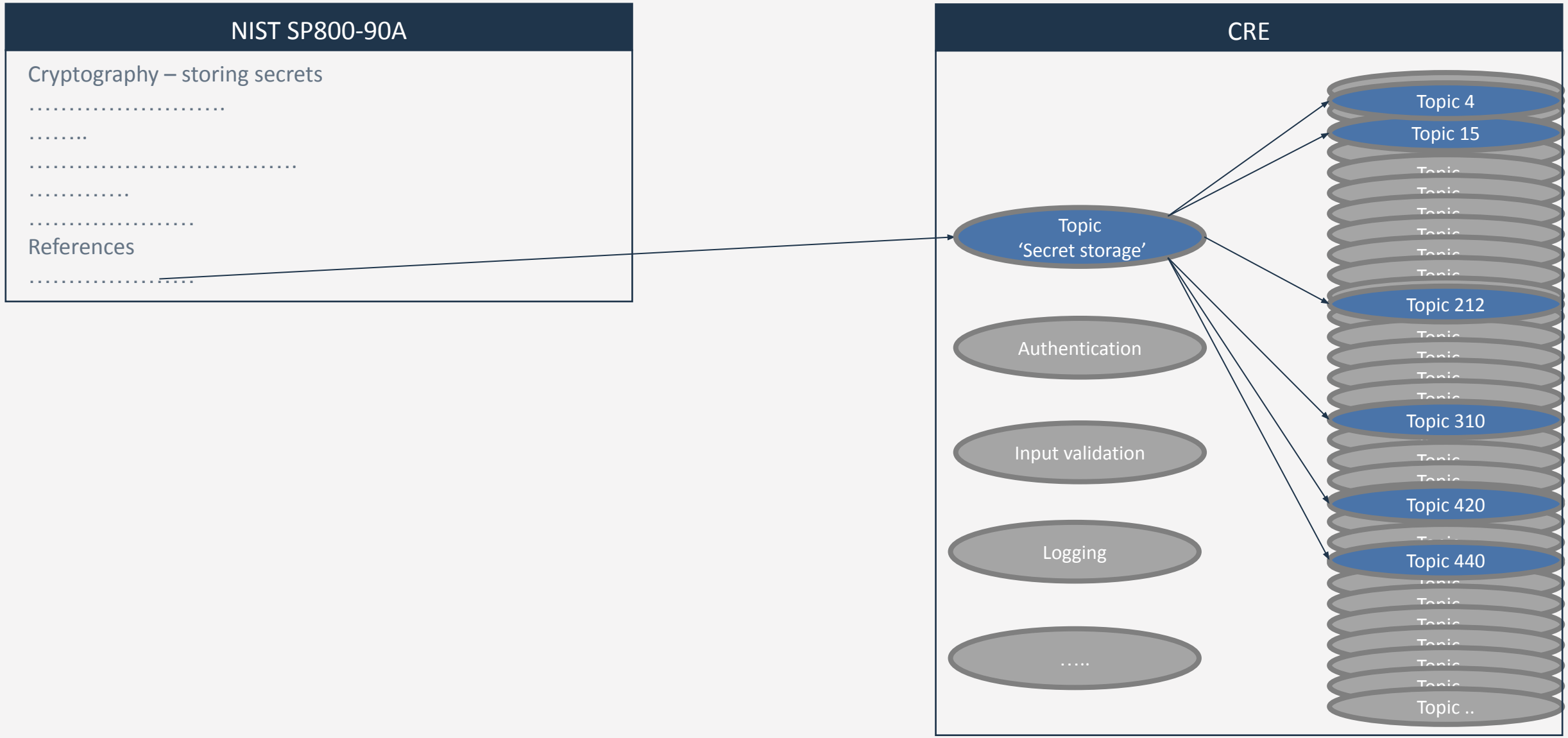
Example of linking to a shared topic



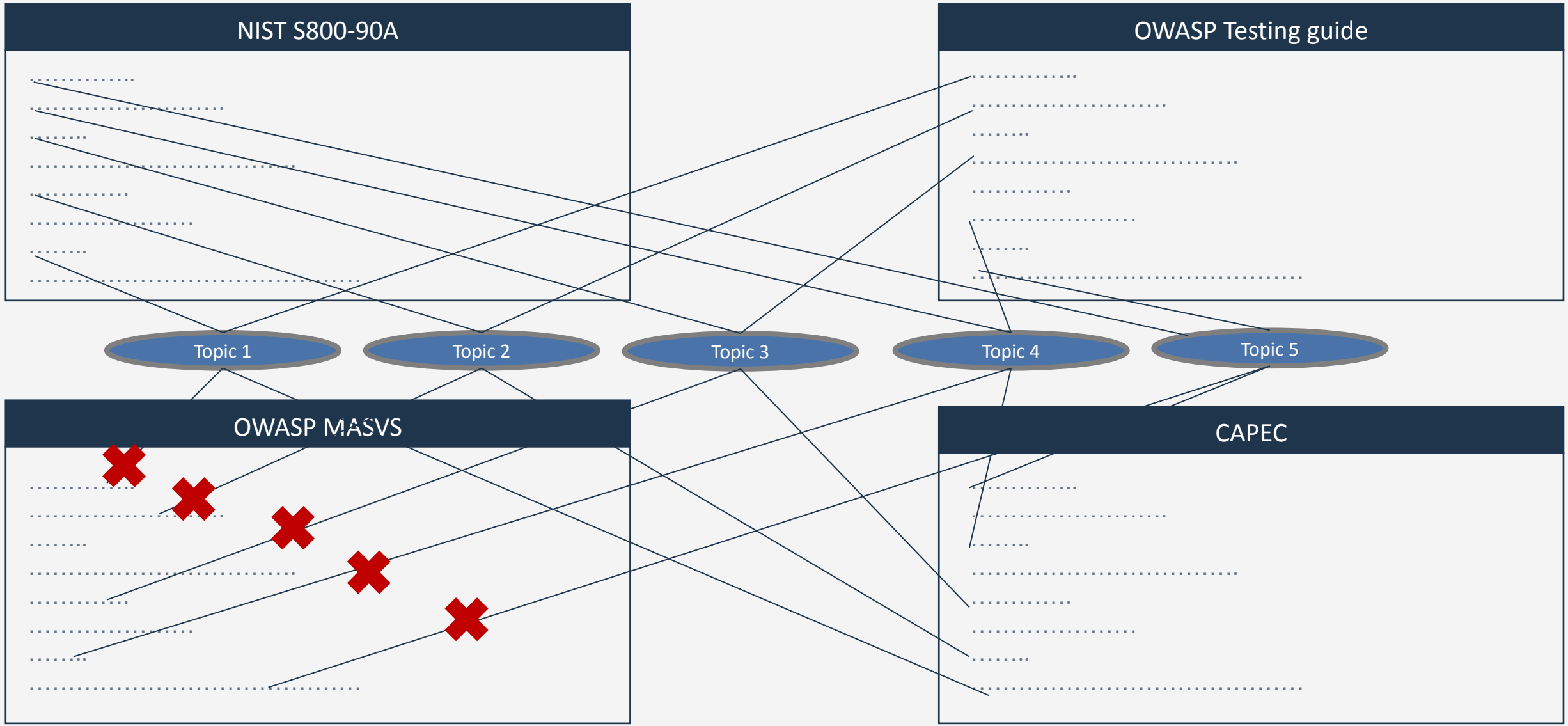
Problem 2: finding all the right topics to link to is unfeasible



Solution 2: higher level topics: easy linking



Problem 3: standards change, so links break



Solution 3: don't map. Make the link from standard to topic the mapping

CAPEC

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

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 without sending user credentials.

125-487

OWASP Testing guide

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

125-487

NIST SP800-90A

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

125-487

Enter the CRE

Designed, implemented and maintained by **Integration standards project** at OWASP:
Spyros Gasteratos, Elie Saad, Rob van der Veer and many friends (kudos to the SKF team)

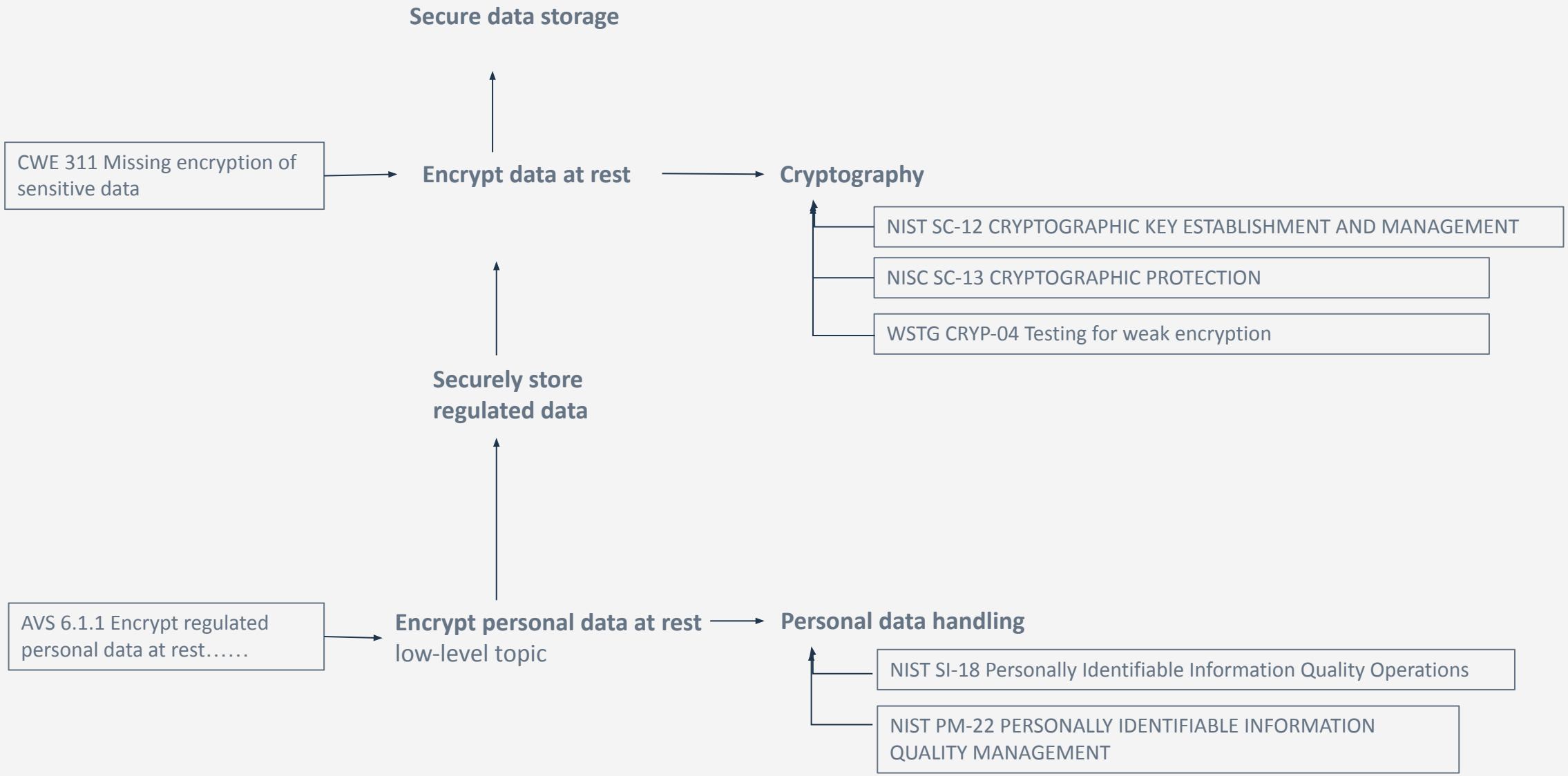
Built on conversations with **stakeholders**: Top 10, ASVS, SKF, OSSF, developers, testers, security professionals etc.

"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."

www.openCRE.org:

- **Mapping**: ASVS, Top10, NIST 63, NIST 53, Pro-active controls, Cheat sheets, WSTG, CWE
- Advanced **linking mechanism**

Example of topic structure: easier linking, and as a bonus: exploration



Demo

Summary

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

- Make it easier for **standard makers** to create and maintain
- Make it easier to **find and use** relevant information for engineers, security officers, testers and procurement

Bonus:

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

CRE Future

1. In progress: alignment with **standard makers and other stakeholders** to connect more standards (now: ZAP, Core ruleset, SKF)
2. **Cool feature ideas**:
    - Gap analysis
    - Graph visualisation
    - Personal profiles
    - Comments
    - Smart ranking with usage data
    - Versioning & snapshots in time

Call to action

Use www.opencre.org and spread the word

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

Thank You!

Questions?