Building Zero Trust Architecture in Public Health

Gesundheitsamt Frankfurt am Main, cronn, ERNW

26/06/2025 – TROOPERS Heidelberg

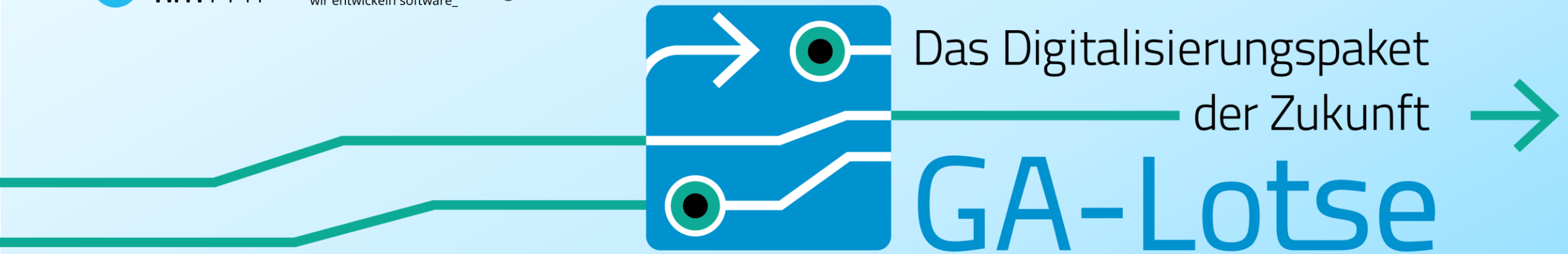
InfoSec IMPACT AWARD

NExT

GESUNDHEITSAMTFFM

cronn wir entwickeln software_

ERNW providing security.



Cooperation:

GESUNDHEITSAMTFFM

HESSEN
Hessisches Ministerium für Familie, Senioren, Sport, Gesundheit und Pflege

Funded by the European Union
NextGenerationEU

Agenda

Das Digitalisierungspaket der Zukunft
GA-Lotse

1. Introduction & Project Context
2. GA-Lotse Architecture and Zero Trust
3. Secure Software Development Life-cycle
4. Implementation & Testing
5. Conclusion

Cooperation:
GESUNDHEITSAMT FFM
HESSEN
Hessisches Ministerium für Familie, Senioren, Sport, Gesundheit und Pflege
Funded by the European Union
NextGenerationEU

Introduction

Bianca Kastl
Gesundheitsamt Frankfurt

Product Owner “GA-Lotse”

Sven Nobis
ERNW Enno Rey Netzwerke GmbH

Security Consulting

Benedikt Waldvogel
cronn GmbH

Lead Software Architect

Project Context and Challenges

- Usually data with a high to very high protection level (Art. 9 GDPR)
- Most of the time Personally Identifiable Information (PII)
- Sometimes anonymous data because of discrimination risk (HIV)
- Sometimes even more secured data (socio-psychiatric service)

Cooperation:
GESUNDHEITSAMT FFM
HESSEN Hessisches Ministerium für Familie, Senioren, Sport, Gesundheit und Pflege
Funded by the European Union NextGenerationEU

Vision

- Learnings from the pandemic
  - IT and workplace has to be more flexible
  - Remote and mobile work becomes more important

→ Zero Trust a new security paradigm that enables a modern workplace

GA-Lotse

Anmeldung mit Passkey

Anmelden mit Passkey

Financial Backing

- Entire project is funded by public money with around 23 million Euro
  - Funding requirements enforce high bar of data protection and security
  - 15% of the budget must be assigned to security and data protection
- Great opportunity to do security the right way from the start

Cooperation:
GESUNDHEITSAMT FFM
HESSEN Hessisches Ministerium für Familie, Senioren, Sport, Gesundheit und Pflege
Funded by the European Union NextGenerationEU

Guiding Principles

- Security by Design and Default (not just as a buzzword)

  → Dedicated security team for the entire project

  → Dedicated testing team on top of team internal testing

- Privacy by Design (not just as a buzzword)
- Open Source from the beginning

Cooperation:

GESUNDHEITSAMT FFM

HESSEN Hessisches Ministerium für Familie, Senioren, Sport, Gesundheit und Pflege

Funded by the European Union NextGenerationEU

Team Structure

Das Digitalisierungspaket der Zukunft
GA-Lotse

9 Business module teams

Data exchange A	Base module B	Base module C	Base module D	Business module E

Business module F	Business module G	Business module H	Business module I

Cross sectional teams

Test	Security
UX / UI	Scrum

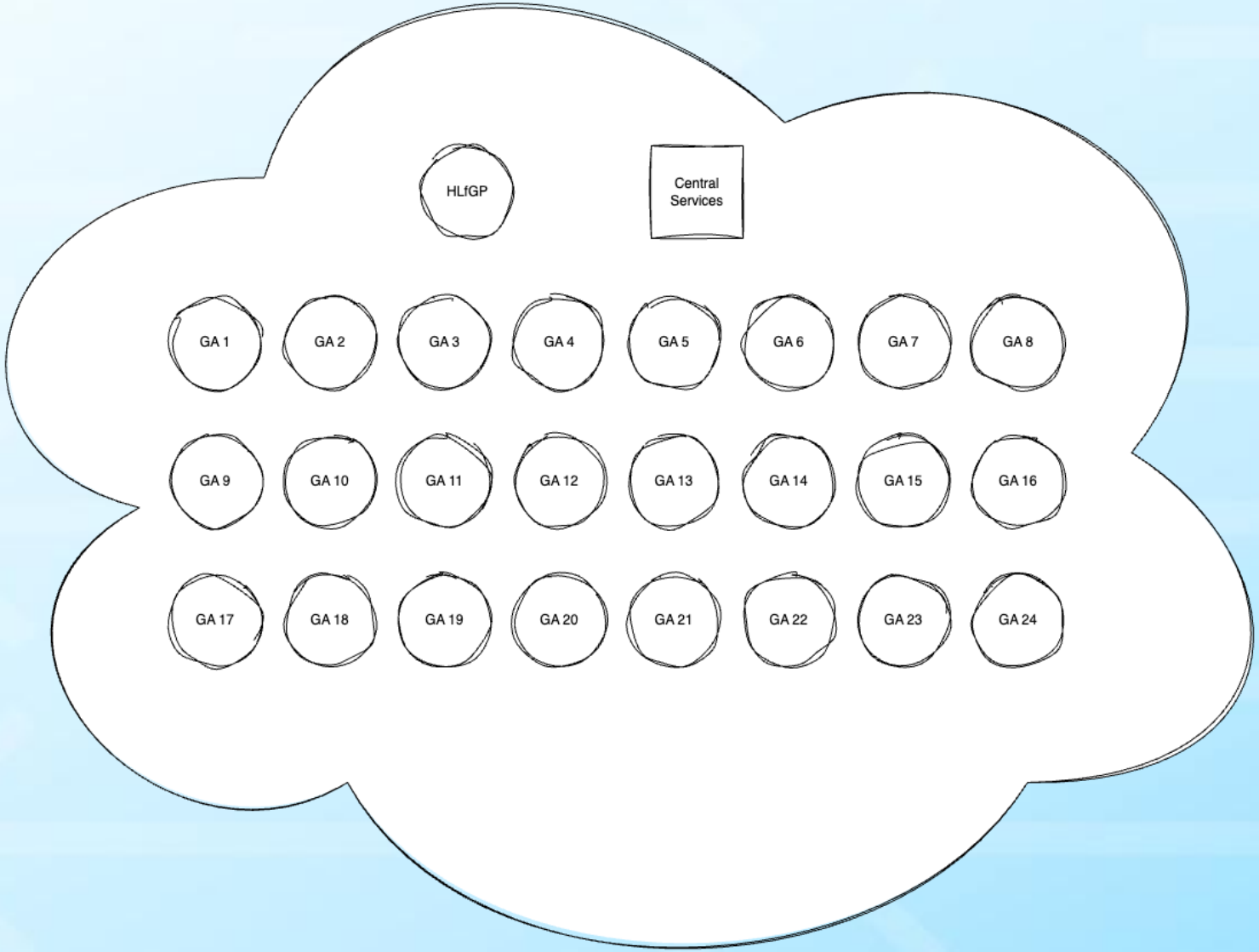
Cooperation:
GESUNDHEITSAMT FFM
HESSEN
Hessisches Ministerium für Familie, Senioren, Sport, Gesundheit und Pflege
Funded by the European Union
NextGenerationEU

Zero Trust Definition

- Minimal privileges – “never trust, always verify”
- There is no “safe environment” anymore

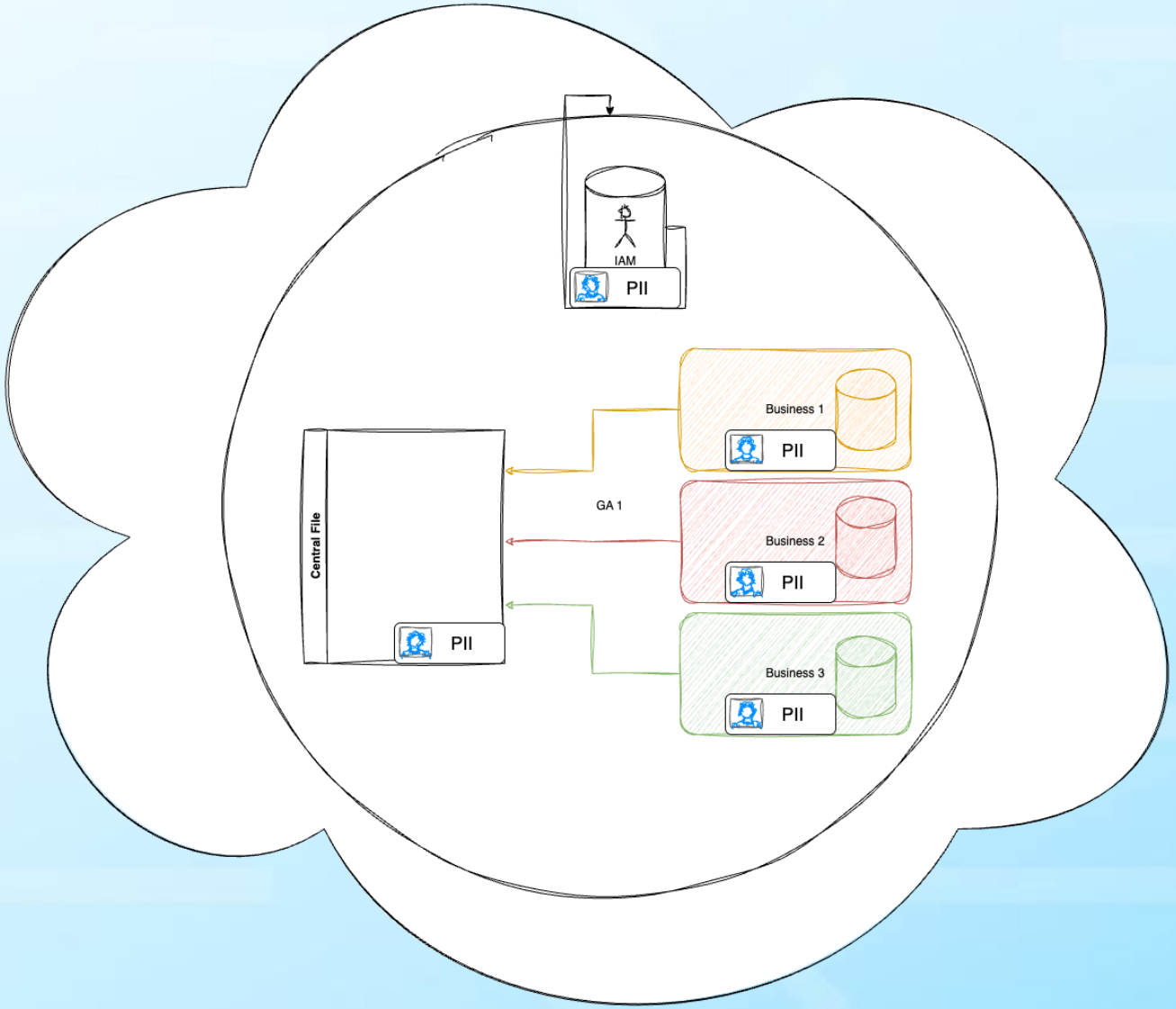
- “Assume Breach”
  - A breach at some time is unavoidable – design systems with a small “blast radius”

Zero Trust Architecture – Segmentation Into Tenants

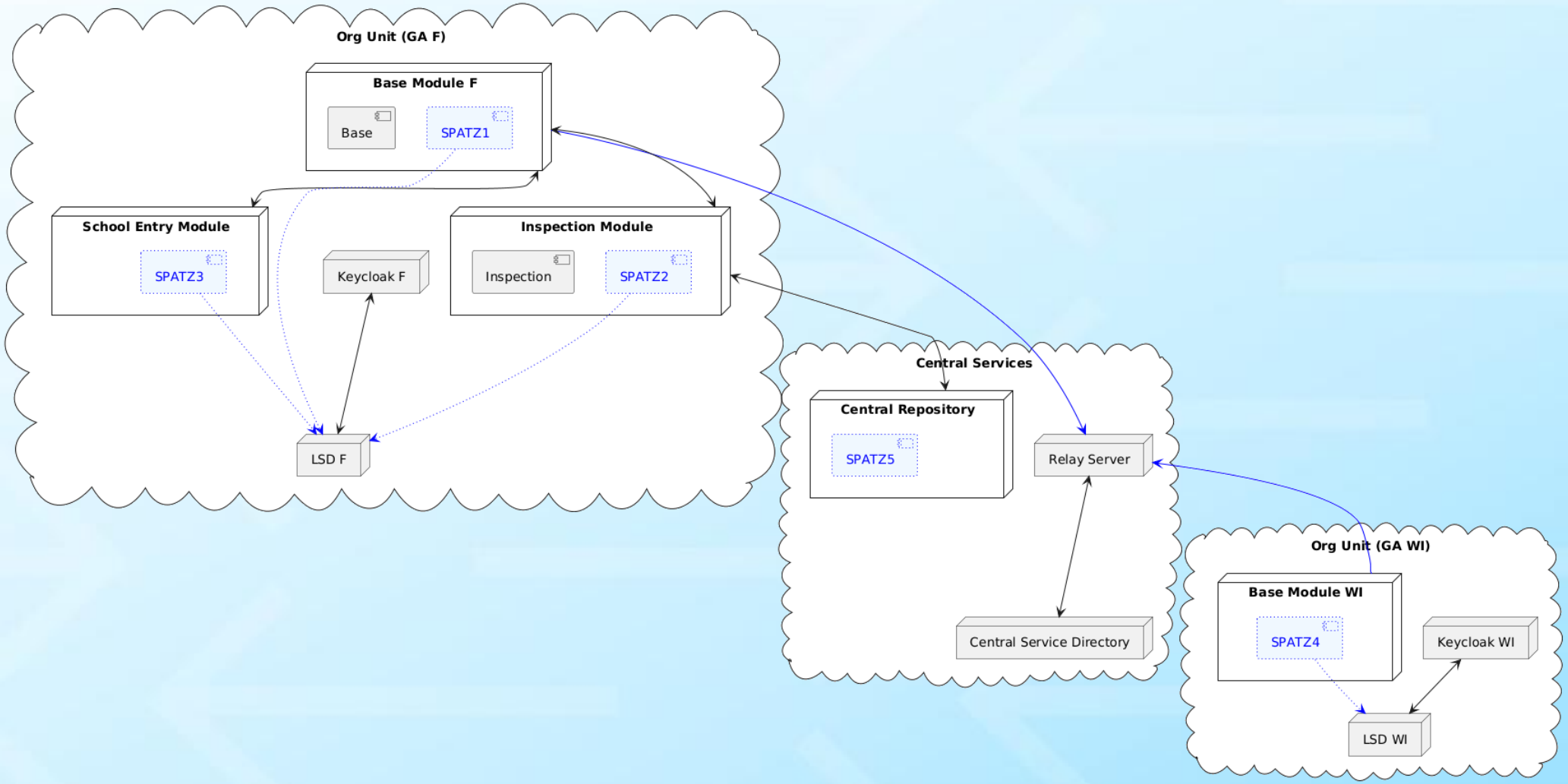


Cooperation:
GESUNDHEITSAMT FFM
HESSEN
Hessisches Ministerium für Familie, Senioren, Sport, Gesundheit und Pflege
Funded by the European Union
NextGenerationEU

Zero Trust Architecture – Segmentation Into Modules



Zero Trust Architecture – Service Mesh (SPATZ)



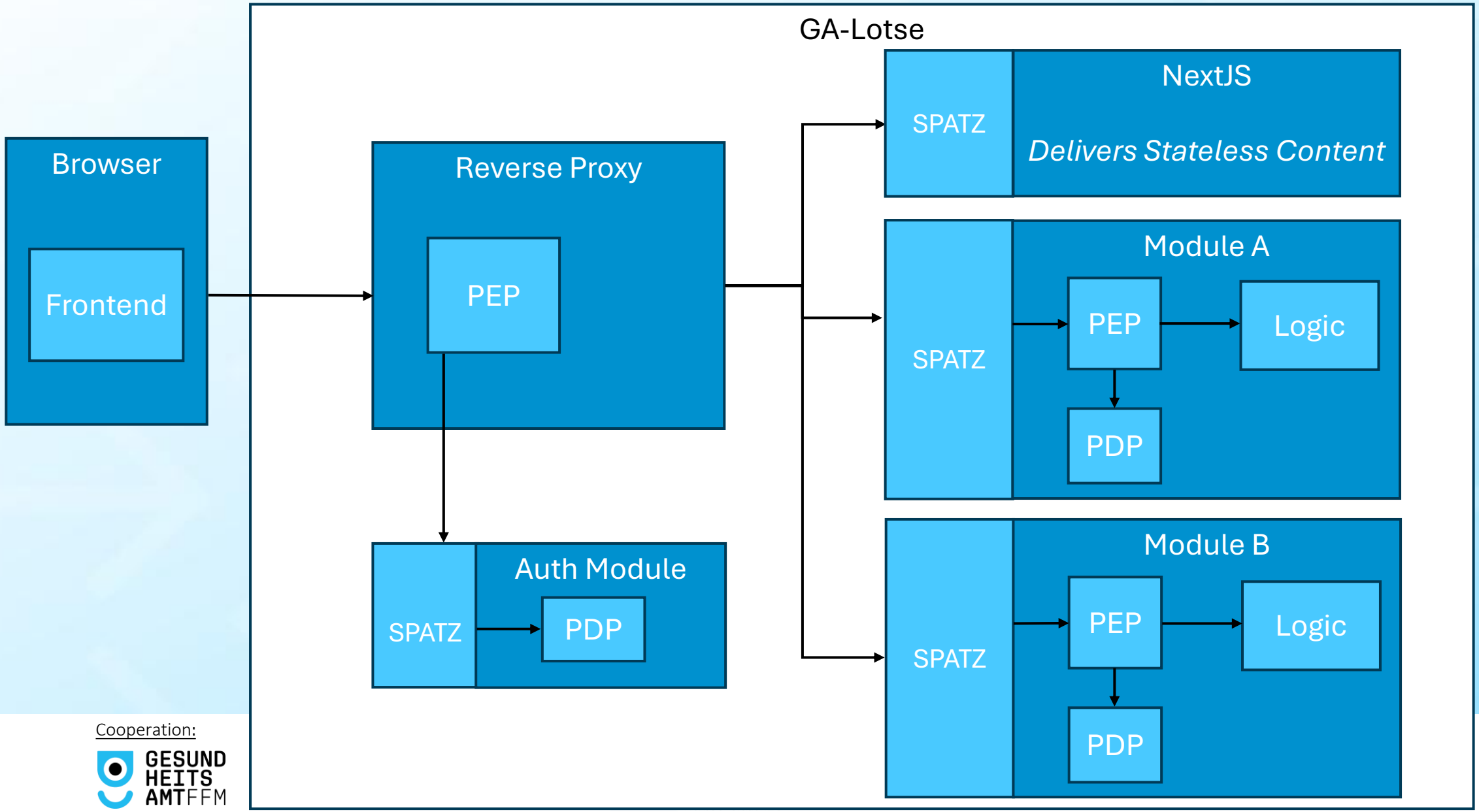
Cooperation:

GESUNDHEITSAMT FFM

HESSEN
Hessisches Ministerium für Familie, Senioren, Sport, Gesundheit und Pflege

Funded by the European Union
NextGenerationEU

Policy Decision & Enforcements Points



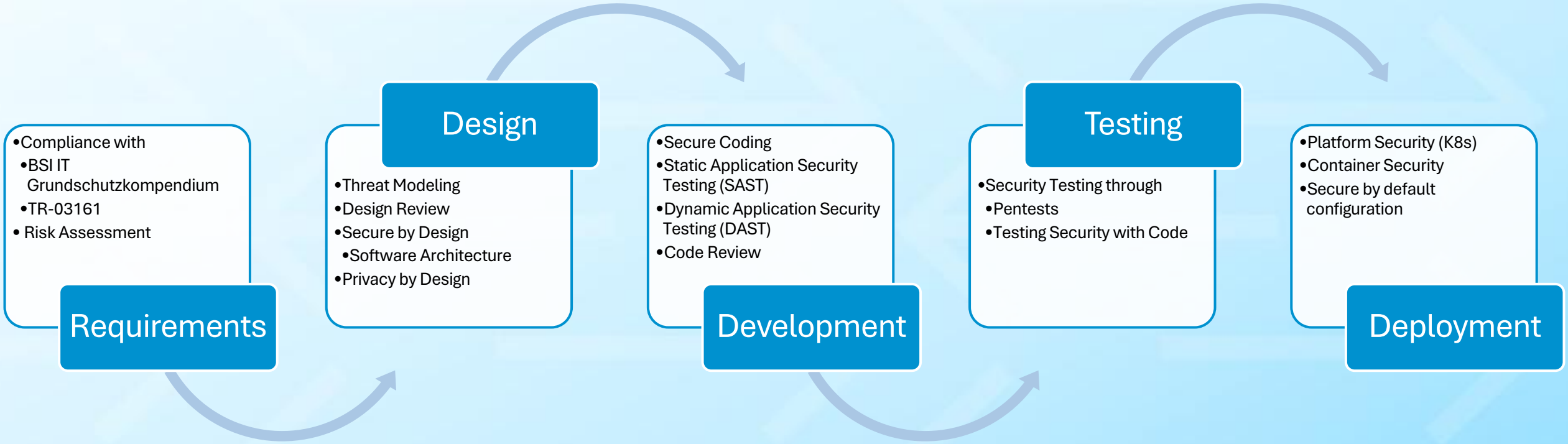
Security in the Software Development Process

Das Digitalisierungspaket der Zukunft
GA-Lotse

- How did we **get to** this secure **architecture**?
- How did we **ensure** that ...
  - ...the **design** has no flaws?
  - ...the **implementation** of this architecture **is secure and accurate**?
- And when should it be done in the development process?
- And finally, what **challenges** did we have?

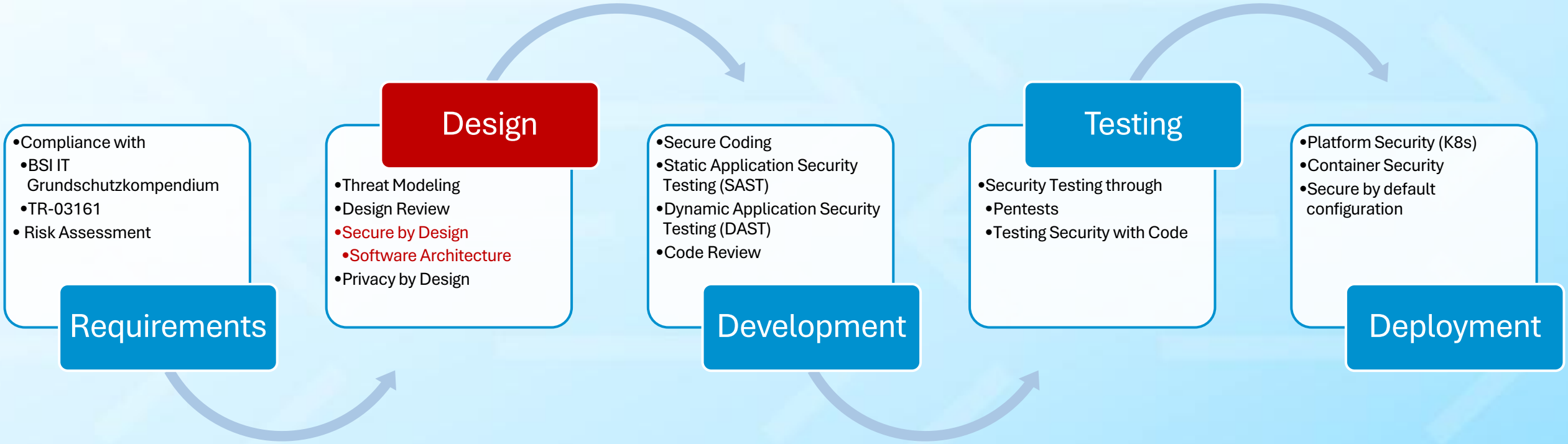
Cooperation:
GESUNDHEITSAMT FFM
HESSEN
Hessisches Ministerium für Familie, Senioren, Sport, Gesundheit und Pflege
Funded by the European Union
NextGenerationEU

Secure Software Development Life Cycle (SSDLC)



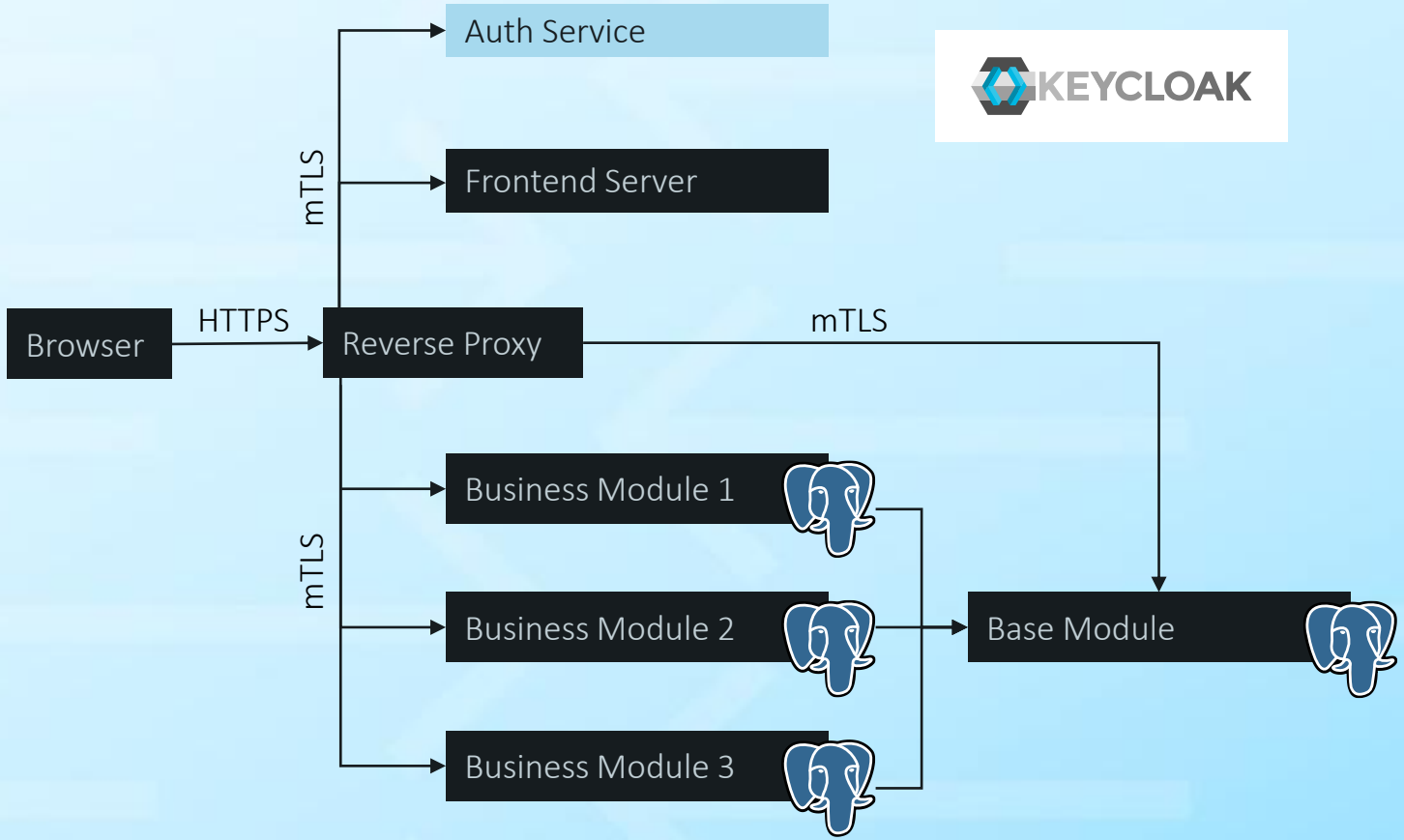
Cooperation:
GESUNDHEITS AMT FFM
HESSEN
Hessisches Ministerium für Familie, Senioren, Sport, Gesundheit und Pflege
Funded by the European Union
NextGenerationEU

Secure Software Development Life Cycle
→ Secure by Design



Software Architecture (Recap)

- Microservices
- Kubernetes
- REST / mTLS



Team Autonomy

Das Digitalisierungspaket der Zukunft
GA-Lotse

Dilemma: Autonomy vs. Centralisation

"9 teams develop

9 solutions

for 1 problem"

Regular consultation between tech leads

Learning:

Enforce rules using ArchUnit!

"hybrid" microservice architecture

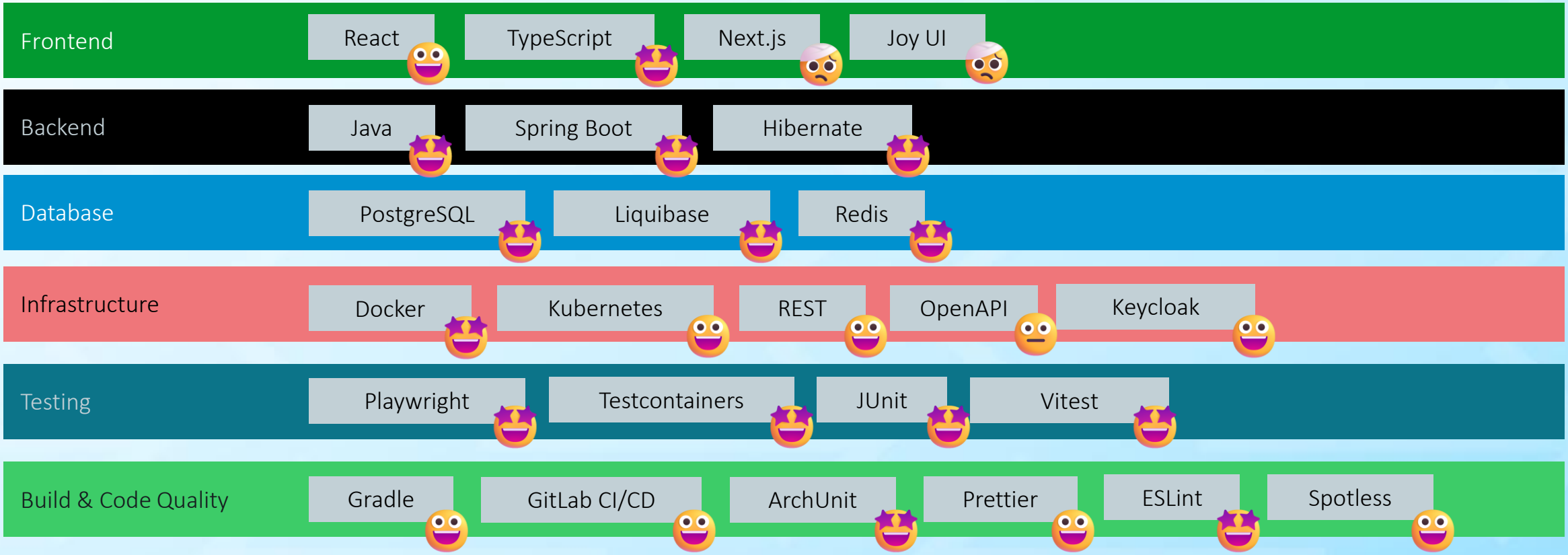
Why?

Reusability!

Unified Tech Stack

Cooperation:
GESUNDHEITSAMT FFM
HESSEN
Hessisches Ministerium für Familie, Senioren, Sport, Gesundheit und Pflege
Funded by the European Union
NextGenerationEU

Tech Stack



Cooperation:
GESUNDHEITSAMT FFM
HESSEN
Hessisches Ministerium für Familie, Senioren, Sport, Gesundheit und Pflege
Funded by the European Union
NextGenerationEU

Choosing the Tech Stack

- Security is only one piece of the puzzle
  - We often fixate on CVEs, but library without maintainers is an equal risk!
- Maintenance & Community
  - **Who's behind it?** Vendor-backed or volunteer?
  - **Is it alive?** Release cadence, open PRs/issues, roadmap
  - **How long does it exist?**
- *Example:* Spring Boot (enterprise stability) vs Next.js (rapid-iterations)
- Developer Experience (DX) often drives decisions

Cooperation:
GESUNDHEITSAMT FFM
HESSEN
Hessisches Ministerium für Familie, Senioren, Sport, Gesundheit und Pflege
Funded by the European Union
NextGenerationEU

Developer Plans vs Privacy Demands

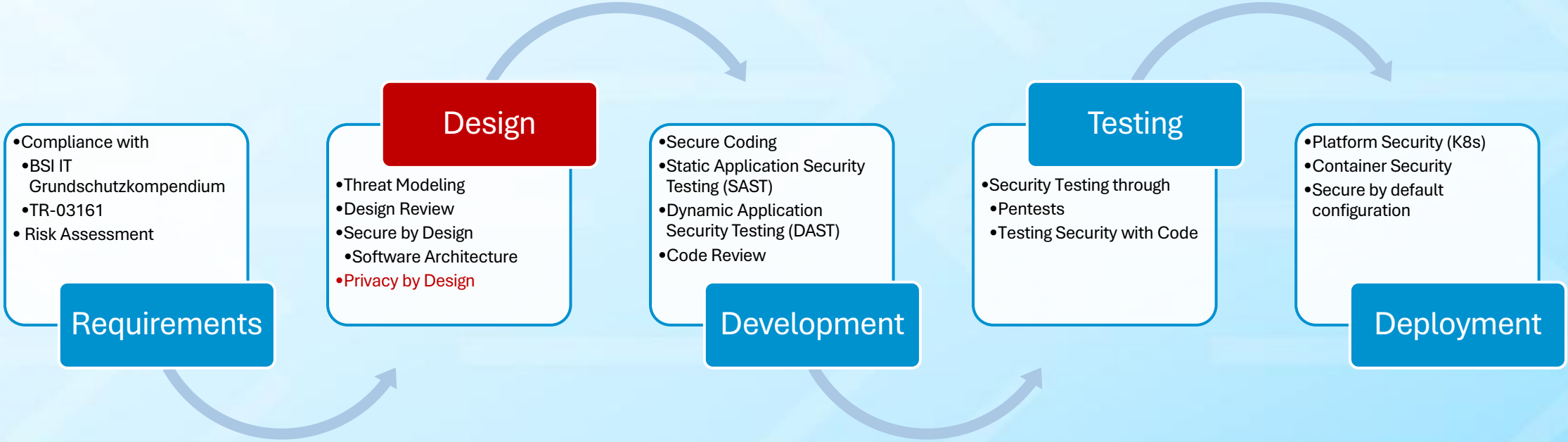
Me (developer)

"Cool: Spring + Hibernate + a DB.
Lets slam in those school entry examinations.
We store person references, how hard can it be? 💪"

Bianca

"Whoa there… remember '**Privacy by Design**':
We don't store anything that lets us actually identify the kiddos ☝️"

Secure Software Development Life Cycle
→ Privacy by Design



Cooperation:
GESUNDHEITSAMT FFM
HESSEN
Hessisches Ministerium für Familie, Senioren, Sport, Gesundheit und Pflege
Funded by the European Union
NextGenerationEU

Privacy by Design: Implementation Challenges (1)

- Case Study: Central File

Base Module		
ID	**Firstname**	**Lastname**
1	Maria	Schmidt
2	Robert	Schmidt
3	Emma	Schmidt
4	Toni	Schmidt

School Entry Module					
Child ID	**Parent 1**	**Parent 2**	**Height [m]**	**Weight [kg]**	**Language Proficiency**
3	1	2	1,15	20,5	Excellent
4	1	2	1,20	24,3	Good

Cooperation:
GESUND HEITS AMT FFM
HESSEN
Hessisches Ministerium für Familie, Senioren, Sport, Gesundheit und Pflege
Funded by the European Union
NextGenerationEU

Privacy by Design: Implementation Challenges (2)

- Case specific IDs

Base Module

ID	Firstname	Lastname
6d28	~~Maria~~	Schmidt
529e	~~Robert~~	Schmidt
91e9	Emma	Schmidt
1762	Toni	Schmidt

Person ID	Case ID
6d28	a186
6d28	514d
529e	32f6
529e	ea59
91e9	b920
1762	d514

School Entry Module

Child ID	Parent 1	Parent 2	Height [m]	[…]
b920	a186	32f6	1,15	…
d514	514d	ea59	1,20	…

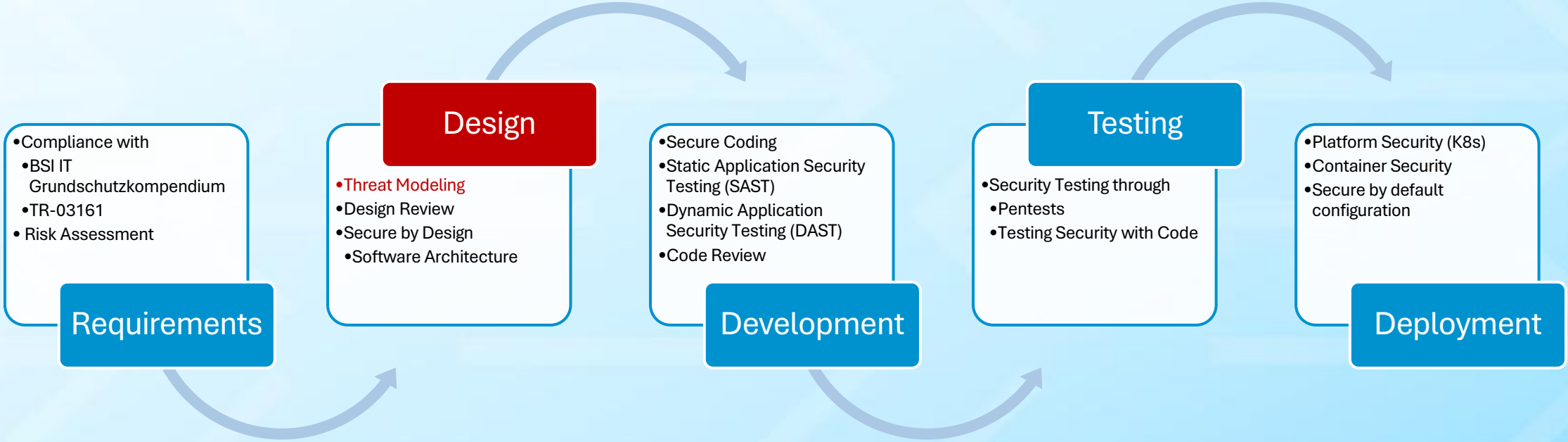
Cooperation:
GESUND HEITS AMT FFM
HESSEN
Hessisches Ministerium für Familie, Senioren, Sport, Gesundheit und Pflege
Funded by the European Union
NextGenerationEU

Privacy by Design: Implementation Challenges (3)

- Zero Trust
  - Attacker with access to school entry DB cannot correlate to real persons
- No (local) DB JOINs!
  - → Remote JOINS via REST requests
    - → Bulk Processing
- Must be implemented from day one

Cooperation:
GESUNDHEITSAMT FFM
HESSEN Hessisches Ministerium für Familie, Senioren, Sport, Gesundheit und Pflege
Funded by the European Union NextGenerationEU

Secure Software Development Life Cycle
→ Threat Modeling



Cooperation:
GESUNDHEITSAMT FFM
HESSEN
Hessisches Ministerium für Familie, Senioren, Sport, Gesundheit und Pflege
Funded by the European Union
NextGenerationEU

Threat Modeling 101

- **High-level goal:** Get a common understanding of the IT security threats in GA-Lotse

- Step 1: Evaluate the threats
  - "What can go wrong?" → threats
  - Use case approach: What can a malicious actor do?

- Step 2: Try to mitigate the risks
  - "What are we going to do about it?"
  → Security by Design, implementation

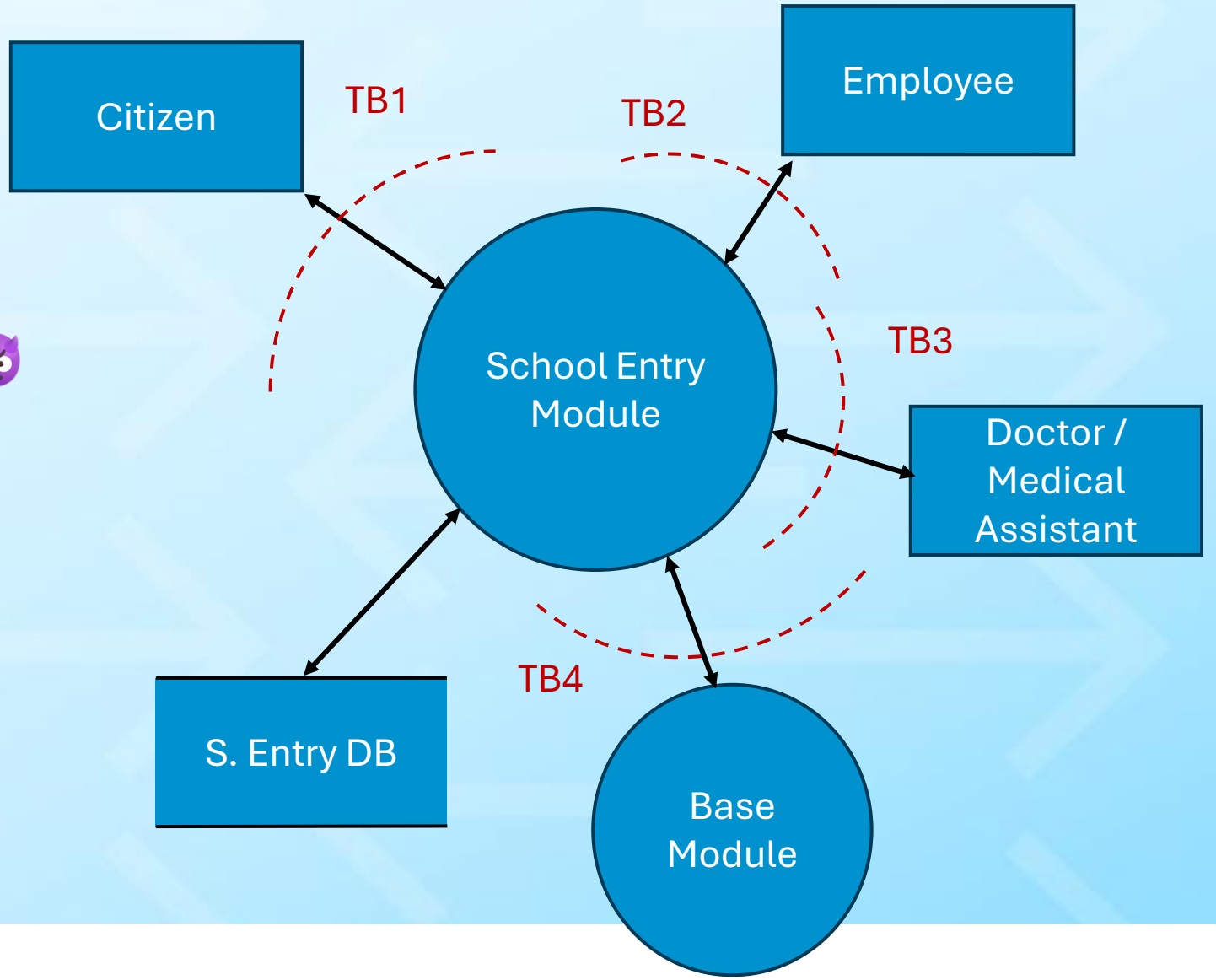
- Step 3: Are the mitigations effective?
  - "Did we do a good enough job?"
  → Code review, security testing: Pentests, security test cases

- *No goal*: domain-agnostic threats (e.g., SQLi, XSS)
  - **Focus is of our TM workshop was:** domain-specific threats

Cooperation:
GESUNDHEITSAMT FFM
HESSEN Hessisches Ministerium für Familie, Senioren, Sport, Gesundheit und Pflege
Funded by the European Union NextGenerationEU

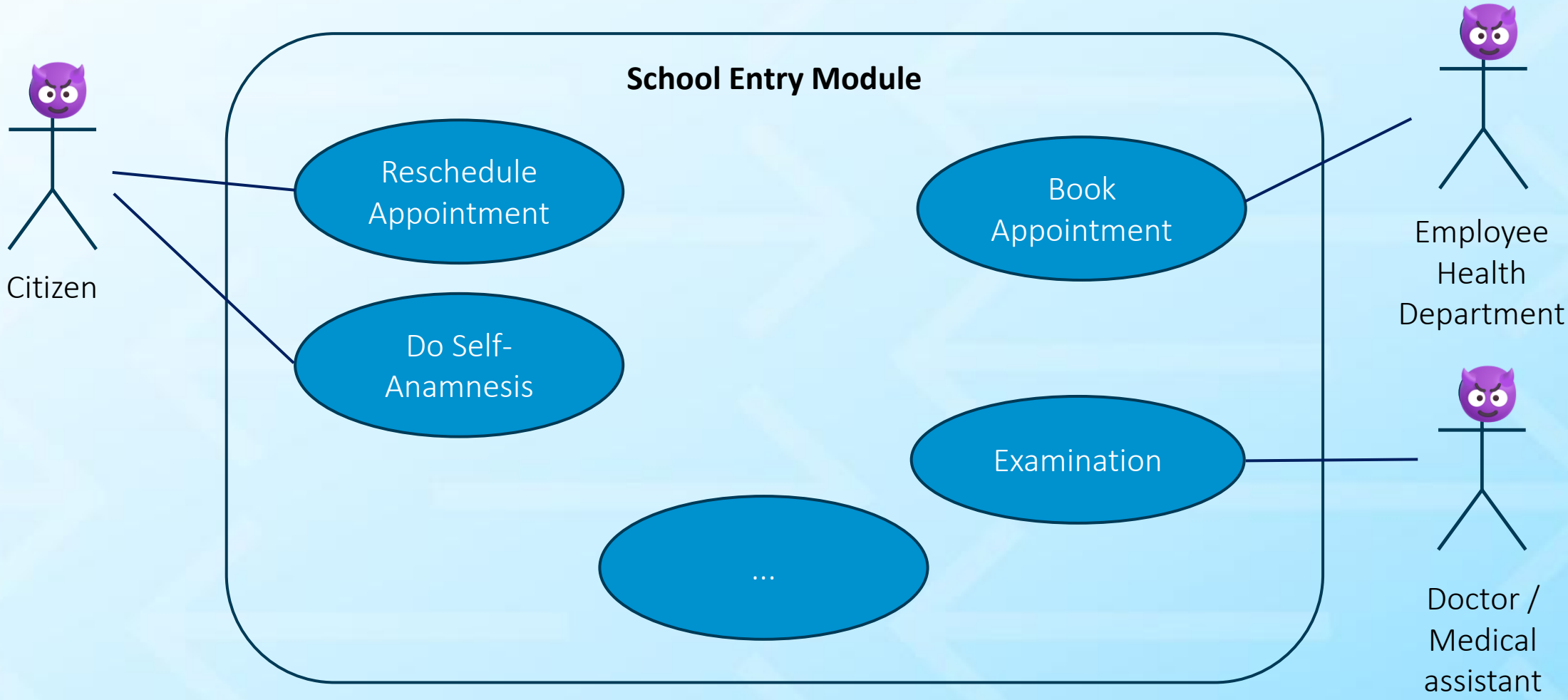
Threat Model in GA-Lotse

- High-Level Threat Model
  - Using STRIDE
- **Use Case Threat Model**
  - Use Case 🙂 → Abuse Case 😈
  - Case Study: School Entry



Case Study: School Entry

Background: Use Cases (Simplified)



Case Study: Self-Anamnesis
Abuse Cases

Das Digitalisierungspaket der Zukunft
GA-Lotse

Domain-Specific Threats

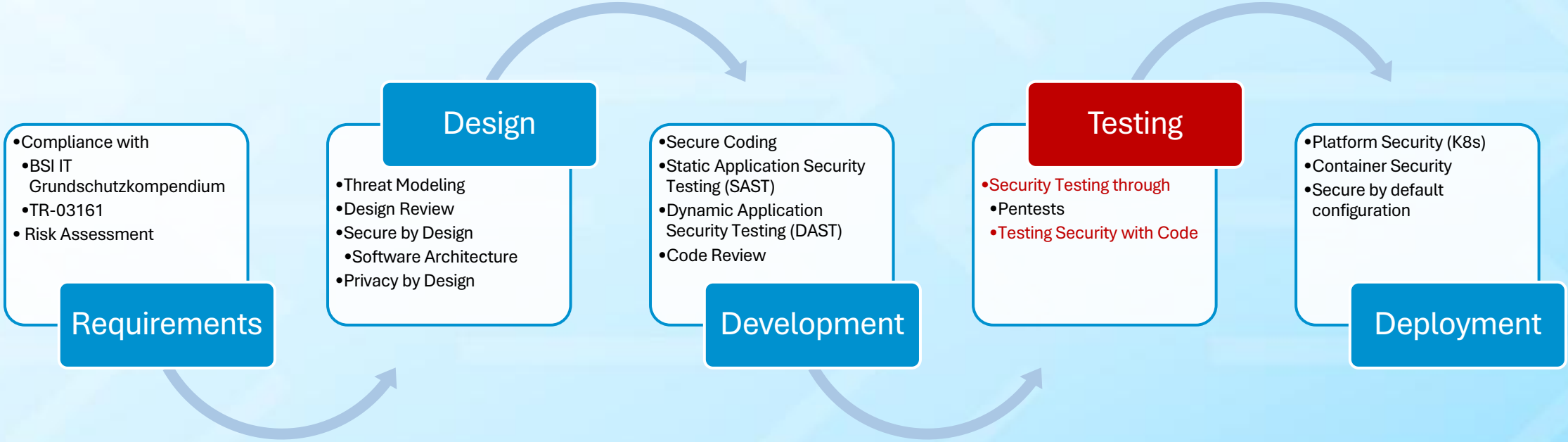
- #1 Attacker finds the invitation envelope in the trash. They use the QR code to access the information provided by the citizen.
  - Mitigation #1: API accepts anamnesis data but does not reveal any data
  - Mitigation #2: Birthday as a second factor (more secure 2nd factors were discussed by not feasible)
- #2 Attacker has access to the citizen's device after they did the anamnesis.
  - …
- #3 Attacker finds the invitation envelope in the trash. They use the QR code to manipulate data.
  - …
- …

Domain-Agnostic Threats

- Spoofing
  - Brute forcing
  - Session stealing
- Tampering
  - Cross-Site Scripting (XSS)
  - Cross-site request forgery (CSRF)
  - SQL-Injection, *-Injection
- Repudiation
  - …
- Information disclosure
  - …

Cooperation:
GESUNDHEITSAMT FFM
HESSEN
Hessisches Ministerium für Familie, Senioren, Sport, Gesundheit und Pflege
Funded by the European Union
NextGenerationEU

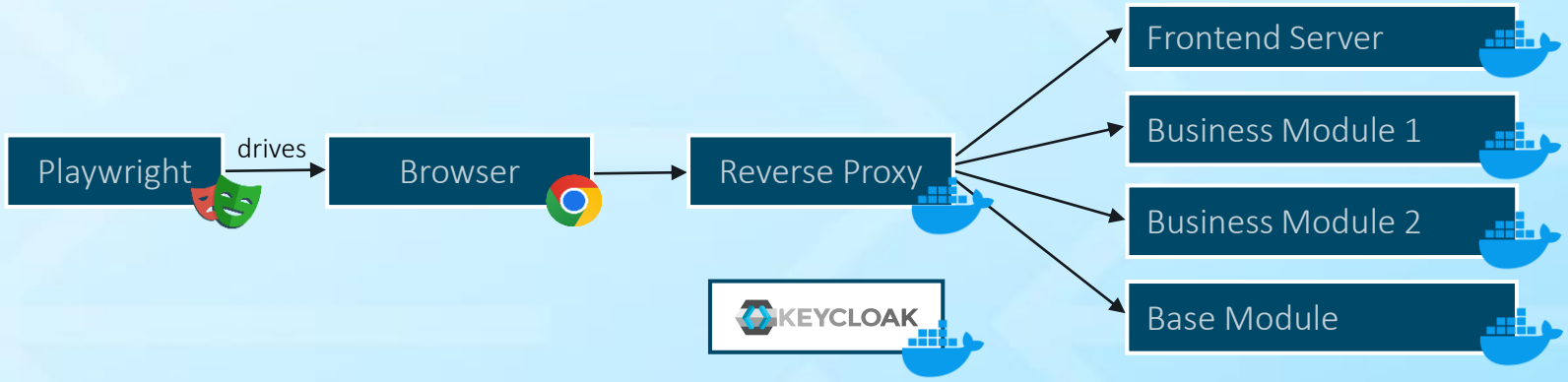
Secure Software Development Life Cycle
→ Secure by Design



Cooperation:
GESUNDHEITSAMT FFM
HESSEN
Hessisches Ministerium für Familie, Senioren, Sport, Gesundheit und Pflege
Funded by the European Union
NextGenerationEU

Testing Approach

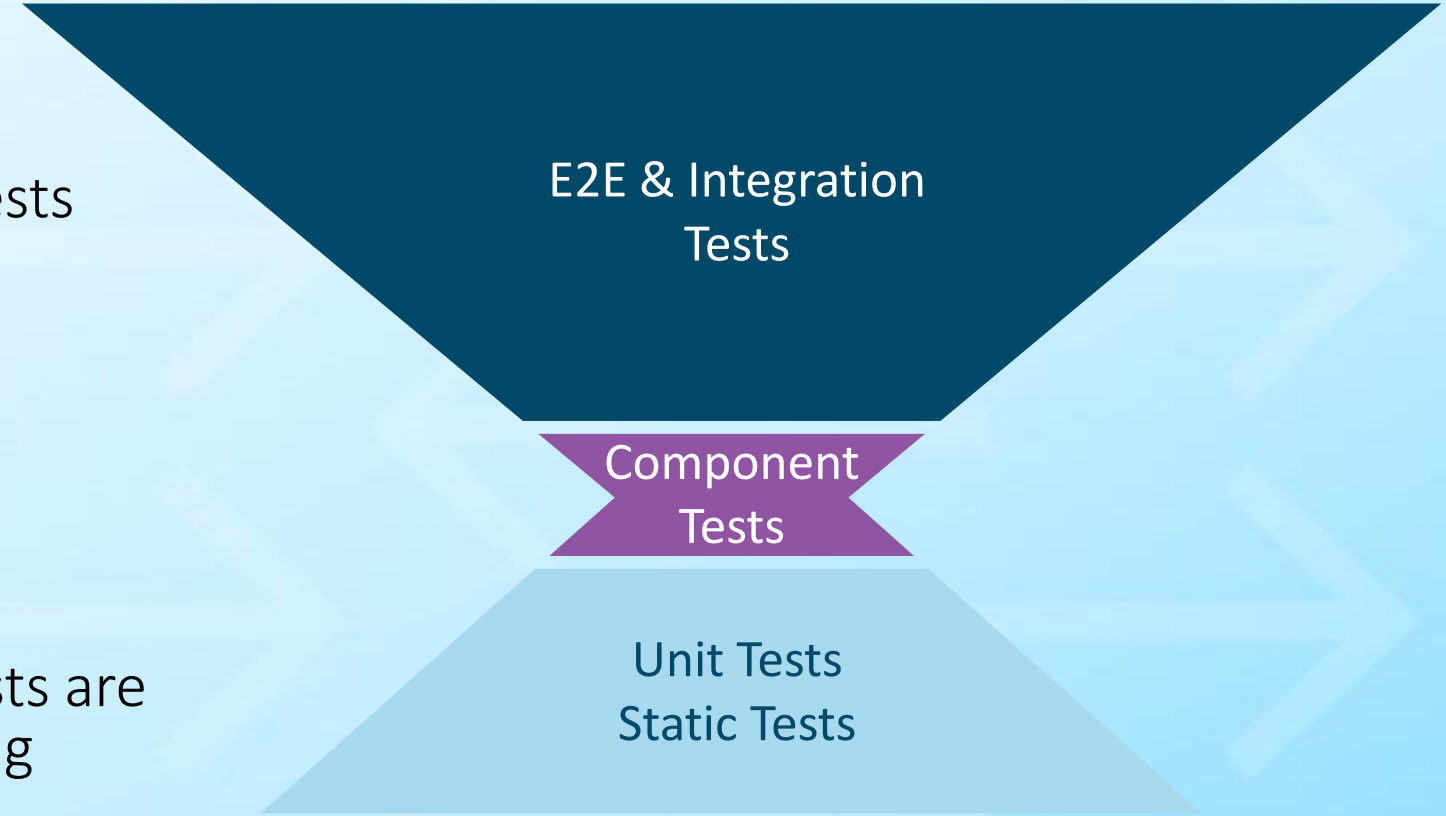
- **Strong focus on integration tests:** Test services together, not in isolation
- **Gradle-driven automation:** Build & launch required services per test run
- **Backend:** JUnit integration tests via REST APIs
- **End-to-end tests:** Playwright drives a real browser against the UI



Testing Trophy Instead of Pyramid

Das Digitalisierungspaket der Zukunft
GA-Lotse

- Many **integration tests**
  - **720** E2E test scenarios
  - **10 000** backend integration tests
- Some **unit tests** & static checks
- Few **component tests**
- (Almost) **no mocking**
- **Why?**
  - Spring service/component tests are maintenance nightmare during refactorings



Cooperation:
GESUND HEITS AMT FFM
HESSEN
Hessisches Ministerium für Familie, Senioren, Sport, Gesundheit und Pflege
Funded by the European Union
NextGenerationEU

Testing: Validation Files

- Aka Snapshot Testing
- Reveals unintended side-effects
- Good fit for **security tests**

```java
@Test
void testNotAuthenticated() {
  CreateProcedureRequest request = new CreateProcedureRequest(…);

  ResponseEntity<String> response =
      testRestTemplate.postForEntity("/school-entries", request, String.class);

  assertThat(response.getStatusCode()).isEqualTo(HttpStatus.UNAUTHORIZED);
  assertHeadersWithFile(response);
}
```

data/test/validation/**testNotAuthenticated_headers.txt**

```
Cache-Control: [no-cache, no-store, max-age=0, must-revalidate]
Cross-Origin-Opener-Policy: [same-origin]
Cross-Origin-Resource-Policy: [same-origin]
Expires: [0]
Pragma: [no-cache]
Strict-Transport-Security: [max-age=31536000 ; includeSubDomains]
Transfer-Encoding: [chunked]
WWW-Authenticate: [Bearer]
X-Content-Type-Options: [nosniff]
X-Frame-Options: [DENY]
```

Security Testing (1)

Das Digitalisierungspaket der Zukunft
GA-Lotse

```java
@Test
void testLogin() {
  HttpCookie sessionIdCookie =
      loginAndAssertResponsesWithValidationFile("/some-path");
  assertRedisSessionStateWithFile(sessionIdCookie);
}
```

data/test/validation/**testLogin_initialRedirect.txt**

```
Cache-Control: [no-cache, no-store, max-age=0, must-revalidate]
Content-Length: [0]
Cross-Origin-Opener-Policy: [same-origin]
Cross-Origin-Resource-Policy: [same-origin]
Expires: [0]
Location: [https://upstream-host:12345/auth/keycloak]
Pragma: [no-cache]
Set-Cookie: [SESSION=[MASKED]; Path=/; Secure; HttpOnly;
SameSite=Lax]
Strict-Transport-Security: [max-age=31536000 ; includeSubDomains]
```

Cooperation:
GESUNDHEITSAMT FFM
HESSEN
Hessisches Ministerium für Familie, Senioren, Sport, Gesundheit und Pflege
Funded by the European Union
NextGenerationEU

Security Testing (2)

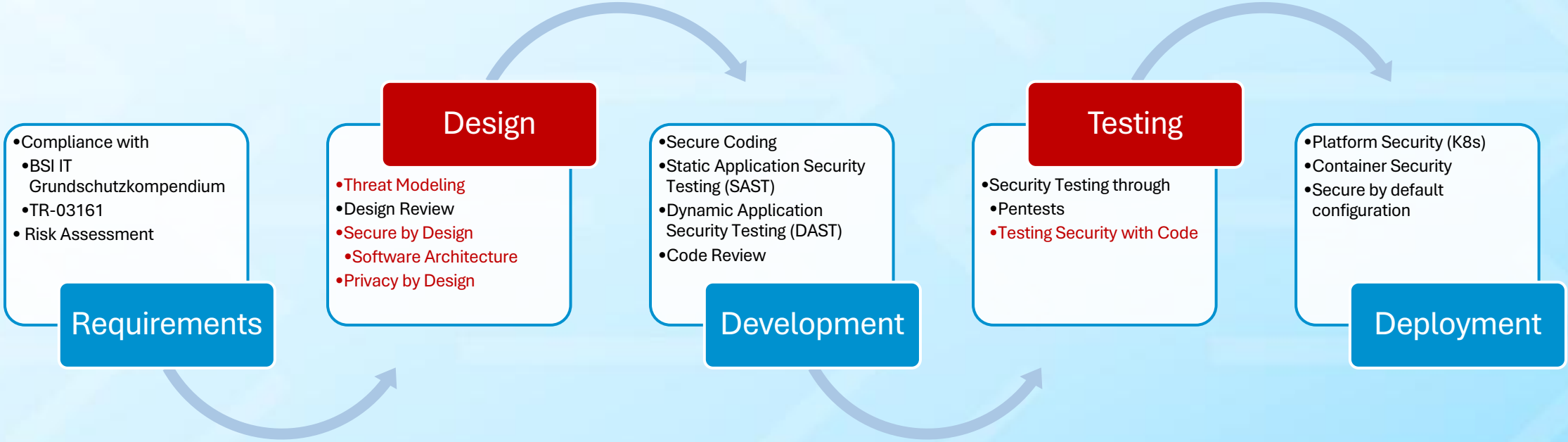
```
class SchoolEntryAuthorizationTest extends AbstractSpringBootTest implements AuthorizationTestTraits {

  @Autowired
  @Qualifier(AuthorizationTestUtil.REQUEST_MAPPING_HANDLER_MAPPING_BEAN_NAME)
  private RequestMappingHandlerMapping requestMapping;

  @Test
  void testEndpointAuthorization() {
    testEndpointAuthorization(testRestTemplate, requestMapping);
  }
}
```

Spring MVC Bean

data/test/validation/**testEndpointAuthorization.md**

METHOD	URL	ALLOWED_ROLES
DELETE	/appointment-blocks/1	SCHOOL_ENTRY_ADMIN
GET	/appointment-blocks/appointment-block-groups	PROCEDURE_ARCHIVE SCHOOL_ENTRY_ADMIN
POST	/appointment-blocks/daily-appointment-block-groups	SCHOOL_ENTRY_ADMIN
POST	/appointment-blocks/daily-appointment-block-groups/validate	SCHOOL_ENTRY_ADMIN
[…]		

Secure Software Development Life Cycle



Cooperation:
GESUNDHEITSAMT FFM
HESSEN
Hessisches Ministerium für Familie, Senioren, Sport, Gesundheit und Pflege
Funded by the European Union
NextGenerationEU

Conclusion

- Creating better and more secure products is possible through a consistent Shift left approach and Zero Trust
- Security problems that are found late in the project are very expensive

Cooperation:
GESUNDHEITSAMT FFM
HESSEN
Hessisches Ministerium für Familie, Senioren, Sport, Gesundheit und Pflege
Funded by the European Union
NextGenerationEU

Contact

Bianca Kastl
Gesundheitsamt Frankfurt
bianca.kastl@stadt-frankfurt.de

Benedikt Waldvogel
cronn GmbH
benedikt.waldvogel@cronn.de

Sven Nobis
ERNW Enno Rey Netzwerke GmbH
snobis@ernw.de

https://gitlab.opencode.de/ga-lotse

Cooperation: