TRAIN

Owner: Jan Rebsch
Reviewer:
Contributors: Andrey Ruzhanskiy, Ivan Gudymenko
Date Generated: Tue Feb 13 2024

Executive Summary

High level system description

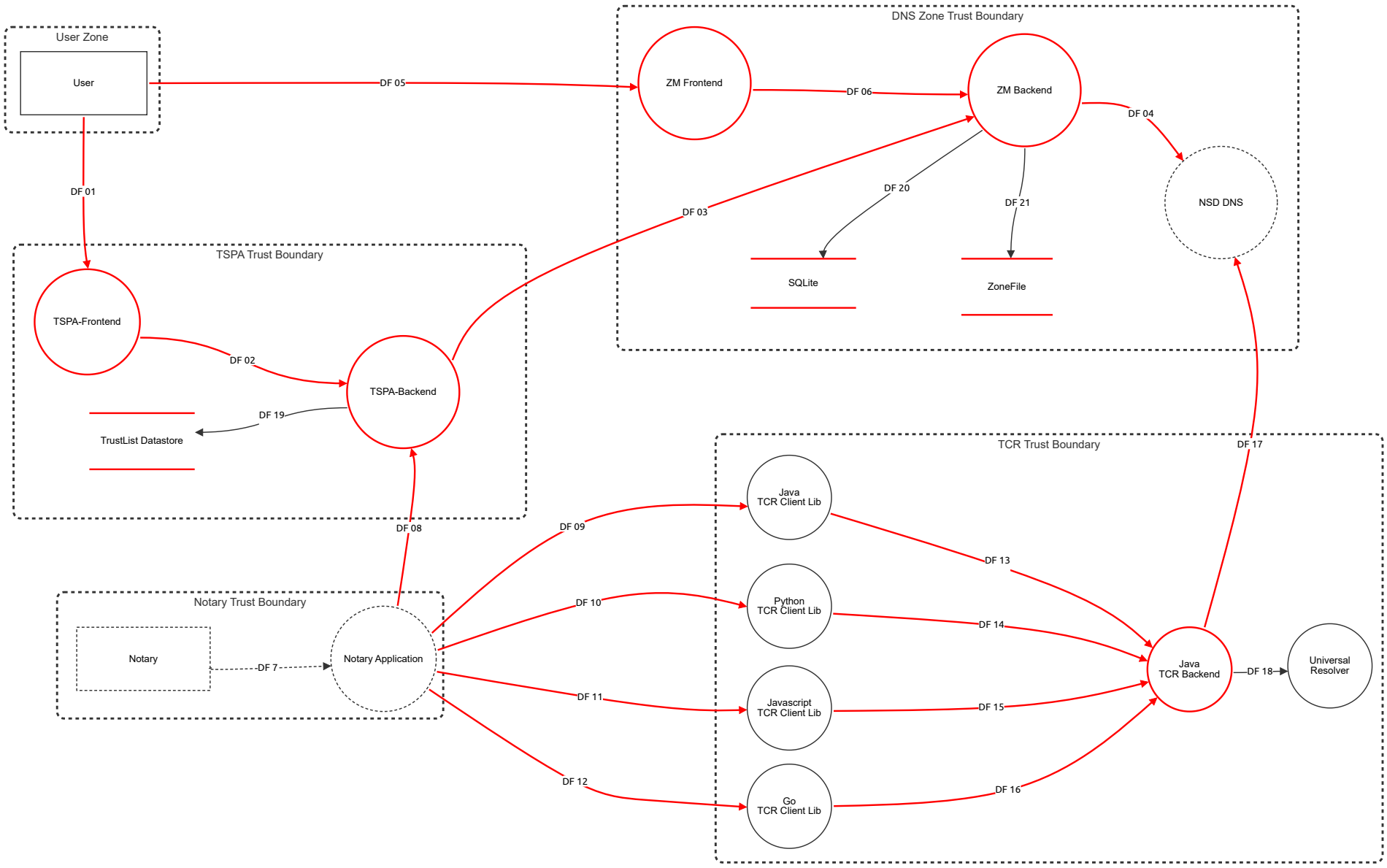
The TRAIN (Trust Management Infrastructure) for Gaia-X will be used to publish lists of trusted entities that are enrolled by a trustable authority. An example could be a specific Gaia-X Federation enrolling its member companies in a member trust list.
TRAIN will allow individual entities (e.g., individual companies, federations that are Gaia-X accredited, federations without Gaia-X accreditation) to make trust statements to support individual trust decisions by sovereign entities. At the same time, depending on individual preference, trust decisions can also be delegated between entities.
TRAIN makes use of the DNS(DNSSEC) as a fundamental and well-established anchor to discover and validate trust. In order for an entity to be able to set up a trust list, it has to control a DNS domain to create a Trust Framework (Trust Scheme) in its DNS record and to set pointers to the Trusted Content, specifically the Trust List, in its DNS record. The DNS hostname is then embedded into the meta section (TermsOfUse) of verifiable credentials by entities claiming enrollment in the Trust Framework of a specific Trust Framework operator. Verifying entities use the DNS hostname to resolve trusted content and validate the inclusion of entities in Trust Frameworks - according to their trust requirements, as they can define which Trust Frameworks (via their DNS hostnames) to trust.

Summary

Total Threats	41
Total Mitigated	4
Not Mitigated	37
Open / High Priority	0
Open / Medium Priority	36
Open / Low Priority	1
Open / Unknown Priority	0

TRAIN-OverView

TRAIN - Decomposition for Threat-Modeling using STRIDE



TRAIN-OverView

User (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

TSPA-Frontend (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
113	Input must be validated	Tampering	Medium	Open		malicious inputs can take advantage of not catched input filters	Inputs need to be filtered to check for malicious code
115	Attacker can pretend to be an admin	Spoofing	Medium	Mitigated		Attacker can pretend to be an admin to gain access to tspa frontend to execute crud	JWT tokens
117	Denial of Service	Denial of service	Medium	Open		An attacker can flood the tspa frontend with requests	deploy via kubernetes use node balancing

TSPA-Backend (Process)

/tspa/v1/{framework-name}/trust-list/tsp
/tspa/v1/init/xml/{framework-name}/trust-list
/tspa/v1/{framework-name}/trust-list/tsp/{id}
/tspa/v1/{framework-name}/vc/trust-list
/tspa/v1/{framework-name}/did
/tspa/v1/trustframework/{framework-name}

Number	Title	Type	Priority	Status	Score	Description	Mitigations
49	Notary Spoofing	Spoofing	Medium	Mitigated		An attacker can impersonate a trusted notary	Use of JWT from a trusted source
50	Manipulate TrustFramework | TrustList | DID Data	Tampering	Medium	Open		An attacker could tamper with: trustframework trustlist dids	https im deployment jwt trusted src
59	Denial of Service	Denial of service	Medium	Open		An attacker can flood TSPA-Backend with request	MUST be deployed in kubernetes
96	Exploit vulnerability	Elevation of privilege	Medium	Open		an attacker can exploit a vulnerability to gain administrative access to the tspa	Provide remediation for this threat or a reason if status is N/A

Notary (Actor) *- Out of Scope*

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Notary Application (Process) *- Out of Scope*

Number	Title	Type	Priority	Status	Score	Description	Mitigations

DF 02 (Data Flow)

HTTP
- Sollte http/s trotzdem sein, wenn über port kommuniziert wird

Number	Title	Type	Priority	Status	Score	Description	Mitigations
119	Denial of Service	Denial of service	Medium	Open		An malicious actor can flood the tspa backend from the frontend by sending a large quantity of requests.	The services need to be deployed using k8s in order to ensure availability.
121	Data flow should use HTTP/S	Information disclosure	Medium	Open		Requests could be intercepted by an attacker.	The requests should require HTTP/S. This will provide confidentiality and integrity. HTTP should not be supported. This should be mitigated by deploying set items K8s and configuring it using best practices

DF 05 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
66	Data flow should use HTTP/S	Information disclosure	Medium	Open		These requests are made over the public internet and could be intercepted by an attacker.	The requests should require HTTP/S. This will provide confidentiality and integrity. HTTP should not be supported. This should be mitigated by deploying set items K8s and configuring it using best practices

DF 04 (Data Flow)

was könnte da im schlimmest fall passieren

selber conatiner

nsd scripte --> das von nsd

selber container wie zm backend

Number	Title	Type	Priority	Status	Score	Description	Mitigations
122	Data flow should use HTTP/S	Information disclosure	Medium	Open		Requests could be intercepted by an attacker.	The requests should require HTTP/S. This will provide confidentiality and integrity. HTTP should not be supported. This should be mitigated by deploying set items K8s and configuring it using best practices

DF 06 (Data Flow)

HTTP-Connection

Number	Title	Type	Priority	Status	Score	Description	Mitigations
120	Data flow should use HTTP/S	Information disclosure	Medium	Open		Provide a description for this threat	The requests should require HTTP/S. This will provide confidentiality and integrity. HTTP should not be supported. This should be mitigated by deploying set items K8s and configuring it using best practices

DF 10 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
81	Dataflow should use HTTP/S	Information disclosure	Medium	Open		These requests are made over the public internet and could be intercepted by an attacker.	The requests should require HTTP/S. This will provide confidentiality and integrity. HTTP should not be supported. This should be mitigated by deploying set items K8s and configuring it using best practices

DF 12 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
79	Dataflow should use HTTP/S	Information disclosure	Medium	Open		These requests are made over the public internet and could be intercepted by an attacker.	The requests should require HTTP/S. This will provide confidentiality and integrity. HTTP should not be supported. This should be mitigated by deploying set items K8s and configuring it using best practices

DF 16 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
126	Data flow should use HTTP/S	Information disclosure	Medium	Open		Requests could be intercepted by an attacker.	The requests should require HTTP/S. This will provide confidentiality and integrity. HTTP should not be supported. This should be mitigated by deploying set items K8s and configuring it using best practices

DF 15 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
125	Data flow should use HTTP/S	Information disclosure	Medium	Open		Requests could be intercepted by an attacker.	The requests should require HTTP/S. This will provide confidentiality and integrity. HTTP should not be supported. This should be mitigated by deploying set items K8s and configuring it using best practices

DF 14 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
124	Data flow should use HTTP/S	Information disclosure	Medium	Open		Requests could be intercepted by an attacker.	The requests should require HTTP/S. This will provide confidentiality and integrity. HTTP should not be supported. This should be mitigated by deploying set items K8s and configuring it using best practices

DF 13
(Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
123	Data flow should use HTTP/S	Information disclosure	Medium	Open		Requests could be intercepted by an attacker.	The requests should require HTTP/S. This will provide confidentiality and integrity. HTTP should not be supported. This should be mitigated by deploying set items K8s and configuring it using best practices

DF 18 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

DF 17 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
54	Data flow should use HTTP/S	Information disclosure	Medium	Open		These requests are made over the public internet and could be intercepted by an attacker.	The requests should require HTTP/S. This will provide confidentiality and integrity. HTTP should not be supported. This should be mitigated by deploying set items K8s and configuring it using best practices
94	An attacker modifies requests	Tampering	Medium	Open		An attcker can intercept an API-Call & modify the data sent by TCR	Provide remediation for this threat or a reason if status is N/A
112	Denial of Service	Denial of service	Medium	Open		An attacker can flood the dns server with requests	Provide remediation for this threat or a reason if status is N/A

DF 01 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
67	Data flow should use HTTP/S	Information disclosure	Medium	Open		These requests are made over the public internet and could be intercepted by an attacker.	The requests should require HTTP/S. This will provide confidentiality and integrity. HTTP should not be supported. This should be mitigated by deploying set items K8s and configuring it using best practices
0	New STRIDE threat	Tampering	Medium	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A

DF 08 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
55	Data flow should use HTTP/S	Information disclosure	Medium	Open		These requests are made over the public internet and could be intercepted by an attacker.	The requests should require HTTP/S. This will provide confidentiality and integrity. HTTP should not be supported. This should be mitigated by deploying set items K8s and configuring it using best practices

DF 03 (Data Flow)

HTTP Access
- Create Trustframework
- Publish DID associated with TrustFramework
- CRUD Ops

Number	Title	Type	Priority	Status	Score	Description	Mitigations
53	Data flow should use HTTP/S	Information disclosure	Medium	Open		These requests are made over the public internet and could be intercepted by an attacker.	The requests should require HTTP/S. This will provide confidentiality and integrity. HTTP should not be supported. This should be mitigated by deploying set items K8s and configuring it using best practices
92	An attacker modifies requests	Tampering	Medium	Open		An attcker can intercept an API-Call & modify the data sent by TSPA	This should be mitigated by using TLS

DF 09 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
80	Dataflow should use HTTP/S	Information disclosure	Medium	Open		These requests are made over the public internet and could be intercepted by an attacker.	The requests should require HTTP/S. This will provide confidentiality and integrity. HTTP should not be supported. This should be mitigated by deploying set items K8s and configuring it using best practices

DF 11 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
78	Dataflow should use HTTP/S	Information disclosure	Medium	Open		These requests are made over the public internet and could be intercepted by an attacker.	The requests should require HTTP/S. This will provide confidentiality and integrity. HTTP should not be supported. This should be mitigated by deploying set items K8s and configuring it using best practices

DF 7 (Data Flow) *- Out of Scope*

Notary as Entity connection

Number	Title	Type	Priority	Status	Score	Description	Mitigations

DF 19
(Data Flow)

Storing TrustList-Data into File

Number	Title	Type	Priority	Status	Score	Description	Mitigations

DF 20 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

DF 21 (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

ZM Frontend (Process)

Read Only

view zone --> ist hardcodes url pfad --> host via env

Number	Title	Type	Priority	Status	Score	Description	Mitigations
129	Denial of Service	Denial of service	Low	Open		An attacker could flood the service with requests to restrict its availability	Use k8s with node balancing as recommended

ZM Backend (Process)

/status
/names/{scheme_name}/trust-list
/names/{scheme_name}/schemes
/view-zone

Number	Title	Type	Priority	Status	Score	Description	Mitigations
56	TSPA Spoofing	Spoofing	Medium	Mitigated		An attacker can impersonate TSPA to create a TrustFramework/ TrustList DID	Use of JWT
61	Denial of Service	Denial of service	Medium	Open		An attacker can flood the TM Backend with requests	Kubernetes deployment with node balancing needs to be implemented
97	User gaining access by explointing a vulnerability	Elevation of privilege	Medium	Open		A user with limited access to the API can discover a vulnerability that allows him to escalate his privileges and gain access to the database and other sensitive data	Deployment with patch policies needed
104	Manipulate intercepted req	Tampering	Medium	Open		an attcker...	Provide remediation for this threat or a reason if status is N/A

NSD DNS (Process) *- Out of Scope*

Third Party not developed by us
kommunikation via ports?

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Java
TCR Client Lib (Process)

finds Trust
accessable by everyone

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Python
TCR Client Lib (Process)

finds Trust
accessable by everyone

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Go
TCR Client Lib (Process)

finds Trust
accessable by everyone

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Javascript
TCR Client Lib (Process)

finds Trust
accessable by everyone

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Java
TCR Backend (Process)

/resolve
/validate

Api endpoints open for everybody
Is used to resolve & validate

Number	Title	Type	Priority	Status	Score	Description	Mitigations
83	TCR Backend receives tampered data	Tampering	Medium	Open		An attacker could send malicious data	use HTTP/S deploy via kubernetes
85	Denial of service	Denial of service	Medium	Open		An attacker could perfrom a (D)DoS Attack in order to restrict the availability	deployment -> nodebalacing

Universal Resolver (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

TrustList Datastore (Store)

TSPA stores TrustList Data into an file

vc signiert
trustlist -> hashed -_> hash ins vc --> vc ist signiert

Number	Title	Type	Priority	Status	Score	Description	Mitigations
65	Unencrypted data	Information disclosure	Medium	Open		An attacker can access TrustListData which is unencrypted	Data should use encrytion
93	An attacker modifies requests	Tampering	Medium	Mitigated		An attcker can intercept an API-Call & modify the data sent by Notary	tl hashed --> hash value im vc --> vc signed

SQLite (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
105	Leakage of secrets	Information disclosure	Medium	Open		Database is not encrypted	Database needs to be encrypted
106	Manipulate Data	Tampering	Medium	Open		redirect data manipulate data	
127	New STRIDE threat	Denial of service	Medium	Open		An attacker could restrict the availability of the SQLite DB	Use of Statefulsets via k8s

ZoneFile (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
107	manipulate zone data	Tampering	Medium	Open		Integrety of data can be compromized from nsd perspective --> requests zonefile	Provide remediation for this threat or a reason if status is N/A