1 MUSIC360 Security Requirements

This section summarizes the requirements concerning security about the Music360 platform. It is based on a series of workshops with the data owners, namely the CMOs and BMAT.

Table 1: Geberal (data) security Requirements

Index	Description
R1	Data custody **OUGHT** to follow the status quo where feasible. Data providers (e.g., CMOs), thus, ought to retain management of the data they currently have custody and control over as to prevent data duplication in domains which are, as of yet, not production tested.
R2	Data providers **OUGHT** to make data in their custody, but owned by other parties, available to the ecosystem, within the reasonable scope of the project's data accessibility requirements.
R3	Data providers **OUGHT** to be empowered to choose which applications (e.g., the dashboard) they serve data to and receive data requests from via a whitelist. N.B., consensus among data providers upon a general whitelist would create the natural boundaries of the Music360 ecosystem but limits its scope until such a whitelist becomes expanded. Such consensus is not necessary but does limit attack vectors.
R4	Data providers **MUST**, where reasonably possible, integrate the software packages provided henceforth with their own systems to make a scope of data in their custody available to the ecosystem where such scope is reasonably required to meet the goals of the research project.
R5	CMOs **MUST** provide means for the following user groups to manage their data: creatives (e.g., artists), venues and policy makers.
R6	Data made available to the ecosystem **MUST** be done so in a secure manner in non-prototype systems (i.e., systems not using mocked data).
R7	Data owner(s) **MUST** be empowered to grant data access to requesting third parties within the ecosystem.
R8	Data owner(s) **MUST** be empowered to revoke data access to third parties.
R9	Data owner(s) **MUST** be warned about the risks of sharing data with third parties in the Music360 ecosystem **PRIOR TO** granting access to such parties.
R10	Data owner(s) **OUGHT** to give their consent and take full liability of the risks associated with data theft from third parties in the Music360 ecosystem.
R11	Access or revocation of data to and from the various parties of the ecosystem **MUST** be done in a timely and consistent manner.
R12	Communication between services in non-prototype systems **MUST** be done over TLS 1.2 or higher.
R13	Provisions against common web attacks (e.g., XSS, CSRF, Injections such as (but not necessarily limited to) SQL Injections, DoS/DDoS) **MUST** be taken by the various components of the ecosystem and documented at a later date in a comprehensive security policy.
R14	Ecosystem database(s), notably, but not limited to, described in D2.1 **OUGHT** to be partitioned in accordance with **R1**.
R15	Ecosystem database(s), notably, but not limited to, described in D2.1 **OUGHT** to be backed up and replicated at a reasonable frequency by the various data providing parties of the ecosystem.
R16	Authorization policies of the ecosystem database(s), notably, but not limited to, described in D2.1 **MUST** be as fine-grained in scope as reasonably possible given the current technological landscape and resource/computation budget.
R17	Ecosystem database(s), notably, but not limited to, described in D2.1 MUST be encrypted using cryptographically secure symmetric or asymmetric algorithms with sufficient collision entropy for the lifespan of the ecosystem; e.g., in the case that at year "n" RSA2048 is not predicted to provide sufficient collision resistance, RSA3072 must be phased in at year "n - (some reasonable time period)".
R18	Ecosystem database(s) OUGHT to phase in homomorphic encryption at such a time when it becomes strategically feasible to increase the security guarantees that the Music360 ecosystem can make.
R19	Encrypted ecosystem database(s) OUGHT to rotate keys at certain intervals under a strict policy in order to prevent data leaks and generally harden security.
R20	A penetration test OUGHT to be taken out by a sufficiently capable actor on a production system with mocked data such that any weaknesses or flaws may be identified and fixed proactively.
R21	Authorization and authentication of the ecosystem MUST be stateless and accomplished in accordance with the JWT standard (RFC 7519, RFC 8725).
R22	For all data providers in the ecosystem, JWTs generated MUST be signed with an asymmetric private key.

Continued on next page

Continued from previous page

Index	Description
R23	For all data providers in the ecosystem, JWTs generated and used by requesting parties MUST provide details of the scope of data access, or can be used to derive scope of data access.
R24	All non-prototype services in the ecosystem MUST be highly available.
R25	All services implementing or working with standards MUST make a best effort to implement best common practices (BCP) where available, moreover, such services MUST also be compliant with data privacy and protection legislation within the jurisdictions they are available in (e.g., GDPR).
R26	Data providers **MUST** reach consensus on a policy for user lifecycle management.
R27	Data providers **MUST** make data accessible in a manner compliant with the FAIR. principles. e.g., Annex A ISO/IEC 27001:2013 section 9.2.

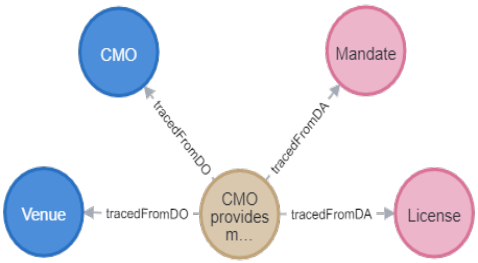

Figure 2: Examples: node SRS_5 traceability mapping in DM-SRS KG

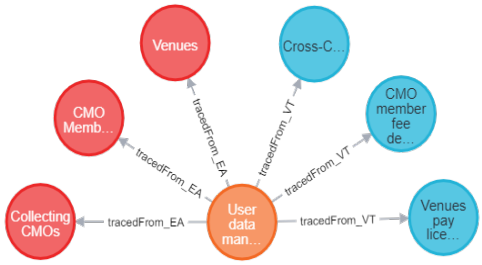

Figure 1: Examples: node SRS_5 traceability mapping in VM-SRS KG

2 Traceability mapping and identified problems

2.1 Traceability analysis between VM and SRS

This part builds a knowledge graph (KG) for traceability analysis between VM and SRS.

2.1.1 KG-based traceability mapping Each VM element (economic actor, value transaction) and SRS item becomes a node (we present the ontologization and instantiation process and examples in sec. **??**). We will execute the traceability mapping by semantic or logic relationships, which serve as edges between these nodes. Based on the ontology of relationship class and their types, we derive and form these trace links. One examples of trace links of SRS_5 to VM is shown and explained in Fig. 1 and explained in Table. 2.

2.1.2 Set of traceability problems Depending on the traceability mapping and analysis we conducted in VM-SRS, the traceability problems can be concluded and listed in Table. 3 from the 4 problem dimensions we defined in Sec. **??**.

2.2 Traceability analysis between DM and SRS

This part builds a knowledge graph (KG) for traceability mapping between DM and SRS.

2.2.1 KG-based traceability mapping Each DM element (data asset, data owner/user, data record) and SRS item becomes a node (we present the ontologization and instantiation process and examples in sec. **??**). We will execute the traceability mapping by semantic or logic relationships, which serve as edges between these nodes. Based on the ontology of relationship class and their types, we derive and form these trace links. One example of trace links of SRS_5 to DM is shown in Fig. 2 and explained in Table. 5.

2.2.2 Set of traceability problems The traceability problems will be identified in Table. 6 from the 4 problem dimensions we defined in sec. **??**.

SRS_5: CMOs **MUST** provide means for the following user groups to manage their data: creatives (e.g., artists), venues and policy makers.

Target Node	Relationship type	Reasoning
EA_2: CMO Members, EA_1: Venues	tracedFrom_EA {type: protects}	SRS_5 protects CMO members/venues to have data management means.
EA_3: Collecting CMOs	tracedFrom_EA {type: constrains}	SRS_5 constrains CMOs to provide data management means.
VT_5: CMO members subscription mechanism, VT_1: Pay Licence fee	tracedFrom_VT {type: supports}	SRS_5 requires data management means to support these two value transactions.
VT_6: Cross-CMO data access	tracedFrom_VT {type: authorizes}	SRS_5 requires authorization for cross-CMO data access.

Problem detected: 1. Policymakers in SRS_5 has not been traced in VM, it should be a missing economic actor.

Table 2: Examples: node SRS_5 traceability mapping in VM-SRS KG

Index	Node involved	Dimension type	Problem description & Improvement suggestion
TP_1	**SRS_11**	AD1: Trace consistency	**VM** - The revocation process has not been marked in the value transaction process between various parties within the ecosystem.
TP_2	**SRS_5**	AD2: Trace completeness	**VM** - Missing economic actor: Policymaker; Missing value transaction path: proof of identification of policymakers ⇔ data access.
TP_3	**SRS_7, SRS_8, SRS_9**	AD2: Trace completeness	**VM** - Missing economic actor: Third-parties; Missing value transaction path: grant proof ⇔ data access.
TP_4	**SRS_14, SRS_15**	AD2: Trace completeness	**VM** - These two SRS items are about database backups and do not reference any specific VM element. This could be considered an untraced requirement from the VM. In practice, they relate to data service components. We can introduce 'Ecosystem database' as a separate economic actor as a VM node.
TP_5	**VT_7, EA_1, EA_5, EA_3**	AD2: Trace completeness, AD4: SRS missing	**VM** - VT_7 states that the experiment will serve as a provided service of the platform, the value transaction path of data sharing from venues has not been shown. **SRS** - Sensitive info shared by venues should be protected in the experiment by privacy preserving computation, corresponding SRS should be specified.
TP_6	**SRS_16, SRS_21**	AD3: Trace redundency	**SRS** - These two SRS items all involve authorization mechanism which can be merged or refined in scope.
TP_7	**VT_2, VT_7, EA_5**	AD4: SRS missing	**SRS** - Audio recognition companies apply fingerprinting to monitor tracks, the hardware-related security and corresponding integration problem with the ecosystem platform has not be specified in security requirements specifications.
TP_8	**VT_7, EA_5, EA_3, EA_4**	AD4: SRS missing	**SRS** - Involves multi-party computation and statistics but lacks SRS trace at the aggregation level. SRS_17, SRS_18 still only focus on the encryption of the database.
TP_9	**VT_5, EA_2, EA_3, EA_4**	AD4: SRS missing	**SRS** - VT_5 states that CMOmembers will register and subscribe platform by default, the informed consent mechanism is not considered in the SRS.
TP_10	**VT_1, VT_2, VT_3, VT_5**	AD4: SRS missing & AD2: Trace completeness	**SRS** - These value transaction path requires a payment process, which may have to integrate some external services like a payment platform, corresponding SRS required. **VM** - A refined value model can include the payment plarform as the economic actor and construct the detailed value tracnsaction path.

Table 3: Traceability problems between VM and SRS

SRS type	Description	Item involved
Confidentially Req. (CR)	Data ownership, sensitive information encryption, secure communication protocol, compliance, etc.	SRS_1, SRS_6, SRS_11, SRS_12, SRS_14, SRS_17, SRS_18, SRS_19, SRS_25, SRS_26, SRS_27
AccessControl Req. (ACR)	User roles, permission control, etc.	SRS_1, SRS_3, SRS_5, SRS_7, SRS_8, SRS_10, SRS_11, SRS_16, SRS_21, SRS_22, SRS_23
DataQuality Req. (DR)	Data availability, data integrity, update frequency, etc.	SRS_2, SRS_4, SRS_6, SRS_11, SRS_13, SRS_15, SRS_20, SRS_24
Transparency Req. (TR)	Record access logs and operational transparency.	SRS_9, SRS_10, SRS_20, SRS_22, SRS_23

Table 4: SRS type classification node hierarchy

SRS_5: CMOs **MUST** provide means for the following user groups to manage their data: creatives (e.g., artists), venues, and policy makers.

Target Node	Relationship type	Reasoning
DA_7: License	tracedFrom_DA {type: protects}	Licenses help to build a data flow between CMO and venues. SRs_5 helps to protect the license data.
DA_8: Mandate	tracedFrom_DA {type: protects}	Mandates help to build a data flow between CMO and rightholders via calims. SRS_5 helps to protect the mandate data.
DO_1: CMO	tracedFrom_DO {type: enforces}	SRS_5 enforces CMOs to provide means of data management liability.
DO_6: Venue	tracedFrom_DO {type: grants_consent}	SRS_5 states licenses from venues grant consent to CMOs to manage their parties' data.

Problem detected: 1. Creatives (e.g., artists) are expressed as rightsholder in DM, resulting in an inconsistency of alignment problem in tracing. 2. The word 'Data' in SRS is not been specified as 'claim', resulting in incompleteness in tracing.

Table 5: Examples: node SRS_5 traceability mapping in DM-SRS KG

Index	Node involved	Dimension type	Problem description & Improvement suggestions
TP_1	**SRS_13**	AD2: Trace completeness	**DM** - Missing data record: Audit & log record.
TP_2	**DR_1: Monitor, DA_10: PerformedPlaylist**	AD4: SRS missing & AD1: Trace consistency	**SRS** - Monitor applies fingerprinting technology to identify music played. Particular SRS should be derived both for device data record (DR_1: Monitor) security and the identified data asset (DA_10: PerformedPlaylist) security.
TP_3	**DO_6: Playlist provider, D0_8: Streaming provider**	AD4: SRS missing & AD1: Trace consistency	**SRS** - The two data owners/users lack coverage in SRS items. **DM** - Owing to these two data owners/users being external service providers outside the MUSIC360 ecosystem platform scope, the necessity of including them in the data model should be investigated further.
TP_4	**DR_3: Statement**	AD4: SRS missing	**SRS** - Non-functional requirements (e.g., report integrity) were omitted.
TP_5	**DR_2: representation**	AD1: Trace consistency	**SRS** - Representation records relationships between an Agent who represents a Claimant in a Claim. It will influence the security schema and scope for Confidentiality Req. and AccessControl Req. in Table. 4.
TP_6	**SRS_12, SRS_13, SRS_14, SRS_15**	AD2: Trace completeness	**DM** - These SRS items are about system configuration (TLS, web-attack protection, database backups) and appear as standalone nodes. For instance, R12 (TLS communication) does not attach to a particular data entity in DM. SRS_14, SRS_15 can be ignored in traced to DM because they can be seen as a high-level requirement for database design. In practice, SRS_12, SRS_13 relate to service components, 'communication services' or 'web attack defend policy' can be extended as data record nodes in DM.

Table 6: Traceability problems between DM and SRS