Audit id, audit record structure and auditable events.

Need to address (CC FAU):

1. Record format – To avoid naming clashes
2. Event selection;
3. Audit log analysis – Audit_id
4. Audit data protection – Either signed by AS to guarantee tamper-proofing, or being encrypted. Also, though outside the scope of this discussion, properly stored so that privileged users cannot tamper with the data;
5. (future) Violation alarms processing – Response system. (Revocation)
6. (future) Audit vs privacy

Audit id

Audit id is a token that's easily processed for audit purposes, so that all participants in the end-to-end conversation (among the audit families and components) would have the same token. The token could be either an alpha-numeric string or a JSON encoded structure.

Participants.

"Main" participants – Resource Server and Authorization Service;
"If desired" - Client, Protective resource and Resource owner. As minimum they should have the ability to get audit id;

Type	**Description**	**Source**	**Examples**
audit ID	Non-modifiable token; Track the participants on all stages of the exchange;	new	"common" token between all related audit families and components (UMA, OIDC etc)
type of event		FHIR	e.g. permissions problem
event category (event action)	Type of action performed when audit generated	FHIR	e.g. RS processing
timestamp	when event was logged	CC FTP_STM	
event outcome	is event reported on success or failure	FHIR	
ip_address/url	of the "host" and the "originator"		
type of source where event originated	Code specifying the type of source where event originated	FHIR	e.g. Client

Resource id	Resource set id	core	
data life-cycle	for the participant object	FHIR	
permission ticket	if applicable	core	
scopes and permissions	what permissions host is looking for, "hoping" permissions etc	Core, Binding 2.3.3	
token status	Full token status	Binding 2.2.4	
RO Access policies		Binding 2.3.1/4, 2.4	
claims	bind identity to claims	Binding 2.2.2/3	
agreed-to obligations		Binding 2.2.1	
skew between permissions validity and actual access		Binding 2.2.1, 2.3.2, 2.4	
role of user	Confidentiality & privacy issues; misuse of the authority	FHIR, CC FAU_GEN.2	e.g. admin, privileged, patient/ doctor
optional	on failure, details of the error and possible fix	CC	

References:

1. http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R4.pdf
   Classes FCO, FDP, FIA and FPR.
2. https://www.hl7.org/implement/standards/FHIR-Develop/securityevent-definitions.html
3. http://docs.kantarainitiative.org/uma/draft-uma-trust.html
4. http://www-01.ibm.com/support/knowledgecenter/#!/SSZSXU_6.2.2.7/com.ibm.tivoli.fim.doc_6227/audit/fimoauth20audit.html
5. http://docs.kantarainitiative.org/uma/draft-uma-core.html
6. http://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7817.pdf