SDP System-level Security View

Document number..... SKA-TEL-SDP-0000013
Document Type..... REP
Revision..... 05
Authors..... R. Simmonds, P. Wortmann, A. Ensor, P. Harding, V. Allan
Release Date..... 2018-04-23
Document Classification..... Unrestricted
Status..... Released

Lead Author	**Designation**	**Affiliation**
Rob Simmonds	SDP DELIV Lead	UCT
Signature & Date:	RWJSimmonds RWJSimmonds (Apr 24, 2018)	

Released by	**Designation**	**Affiliation**
Paul Alexander	SDP Project Lead	University of Cambridge
Signature & Date:	Paul Alexander Paul Alexander (Apr 24, 2018)	

Table of Contents

List of Abbreviations

AAAI	Authorization, Access, Authentication and Identification
CSP	Central Signal Processor
LFAA	Low Frequency Aperture Array
NSDN	Non-Science Data Network
SDP	Science Data Processor
SKA	Square Kilometre Array
SSH	Secure Shell
SRC	SKA Regional Centre
TBW	To be written
TM	Telescope Manager
VPN	Virtual Private Network
WAN	Wide Area Network

1. Primary Representation

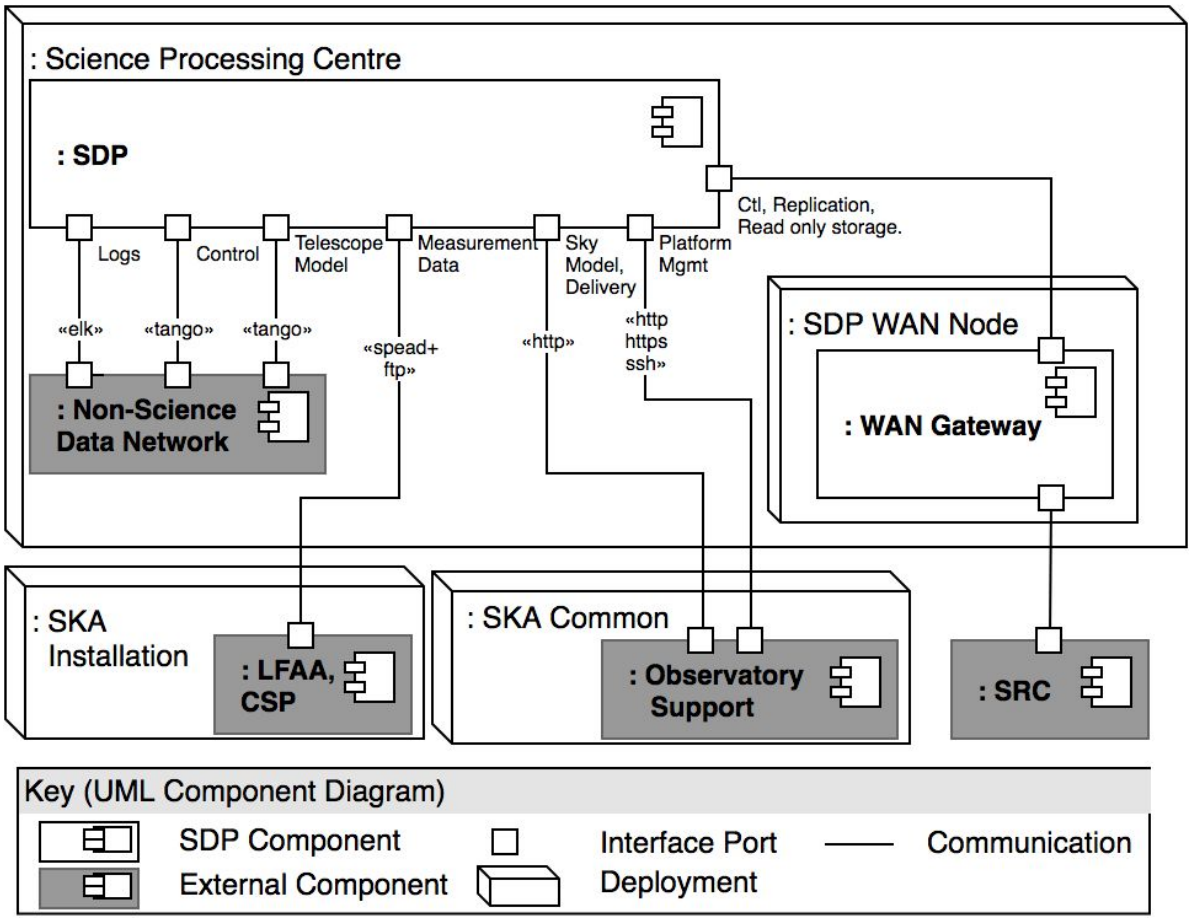

Figure 1: SDP connections to other other components. SDP interaction with SRCs is performed through the SDP WAN Gateway component to isolate the high speed WAN with limited firewalling from the rest of SDP.

The Primary Representation shows the Science Processing Centre that hosts the SDP and the TM. There will be one Science Processing Centre in each of the host countries. Each one will be associated with an SKA Installation site that hosts the LFAA in Australia, and the CSP in South Africa. Each of the SDP sites also connect to SKA Common which will be located at the SKA Headquarters. Also the SDP will connect to SKA Regional Centres (SRCs) through a high bandwidth Wide Area Network (WAN) that will enable the distribution of Science Data Products to the SRCs. A WAN Gateway component provides the interfaces to the WAN.

The SDP connects to other SKA-run systems (e.g. one of the two SDP sites, or the SKA Headquarters) via different networks, and also connects to SRCs through the wide area bulk data network. The networks are

1. a high speed network for ingesting data from the telescope receivers,
2. the Non-Science Data Network (NSDN),
3. the network connecting externally to operations staff not located in the Science Processing Centre and
4. the WAN connecting to the SRCs.

Note that in general AAAI is outside of the scope of SDP. Interfaces will need to be provided by other SKA elements for making calls for user level authentication and authorisation. It is likely that federated identity providers, such as Shibboleth [AD01] deployments will be provided for authentication and role based authorisation services, such as COmanage [AD02], will be provided to service these calls.

2. Element Catalogue

2.1. Elements and Their Properties

To discuss security of elements we identify the following properties per element as cornerstones of the lightweight security discussion in this document:

- **Access:** What actors can access the component/network in question
- **Desired Access:** Which subset of these actors we want to communicate with
- **Disruption Potential:** What damage to the system could be done over this interface
- **Security Measures:** Actions taken to prevent disruption

2.1.1. Science Processing Centre (Management Network)

Access: Anybody with physical access to data-centre / VPN
Desired Access: Internal components, Essential Operations Staff
Disruption Potential: Critical, could affect all components
Security Measures: Basic user/component isolation for robust multi-tenancy

The Science Processing Centre should have strong physical security to prevent the system being compromised by someone accessing an SDP server from a terminal, or connecting to the internal networks. This could be achieved with a secure dedicated data centre, or using a fenced off area in a shared data centre. If an Science Processing Centre local management network needs be be accessed from outside of the physical data centre, this access should be performed over a VPN, access to which is restricted to essential operations staff.

2.1.1. Non-Science Data Network

Access: Anybody with access to data-centre, telescope operators and people with access to the Telescope Manager
Desired Access: Telescope Manager and its authorized users
Disruption Potential: **C**ritical, main control interface
Security Measures: Authenticate TM via TANGO security

The NSDN is used to communicate with TM. The TANGO security layer can help to verify that communications are coming from that system and not from another source that has managed to gain access to this network. However, there will still be risk to SDP if TM becomes compromised and the TANGO security credentials are stolen. Therefore SDP operators need to be informed of any possible compromise of TM as soon as this is detected.

2.1.2. LFAA/CSP (High Speed Ingest Network)

Access: Dedicated ingest network

Desired Access: Just LFAA/CSP
Disruption Potential: Minor, only measurement data
Security Measures: Minimal

The LFAA and CSP will be connected via the high speed ingest network that leads from the SKA dish / antennae Installation sites to the associated SKA data-centre housing the SDP equipment processing data for that site. This network will only be protected by the physical security implemented, and should only expose the services required for the data ingestion tasks required of SDP.

2.1.3. SKA Common (Management Network)

Access: Anybody with physical access to data-centre / VPN
Desired Access: Platform and Scientific operators
Disruption Potential: Critical for SSH access, moderate for delivery interfaces, relatively minor on monitoring interfaces
Security Measures: User authentication and authorization

SKA operators and SKA observatory scientists will connect to the SDP from SKA Common. The interface from SKA Common will require user level authentication and authorisation. Systems for implementing these are outside of the scope of the SDP consortium. It is likely that in most cases these will make calls out to AAAI services running in SKA Common.

2.1.4. SRC (Bulk Data Network)

Access: Sites connected to SRC engineered network
Desired Access: SKA Regional Centres
Disruption Potential: Moderate
Security Measures: WAN Gateway, Host Access Control List, X509 authentication of endpoints

The bulk data transfer network will be used mainly for transferring SDP Data Products to SRCs. The Transfer Endpoint used to perform data transfer will be deployed in a security zone that has read only access to SDP storage. Authentication and Authorisation for these endpoints will most likely be provided using X509 service certificates associated with particular SRCs.

Auditing of exactly who at an SRC requested a particular product would be handled by the SRC and made available to the SKA on request. A separate security zone within the WAN Gateway will run the Regional Centre Access component via an SRC operator which is authorised to request SDP Data Products and monitor the progress of transfers to their site.

2.2. Relations and Their Properties

Not applicable

2.3. Element Interfaces

Interfaces between elements (TM, SDP, LFAA, CSP) are described in the relevant ICDs listed below. The interface to the SRCs has not been written yet. Pragmatically in terms of security architectures, the interfaces between deployments will be more pertinent, and this has been described below the Primary Representation.

CSP: The interface to CSP is described in the documents 300-000000-002_04_MID_SDP-CSP-ICD and 100-000000-002_04_LOW_SDP-CSP-ICD (Mid and Low respectively). [RD03]

LFAA: The interface to LFAA is described in 100-000000-033_01_LOW_SDP-LFAA-ICD. [RD04]

TM: The interface to TM is described in the 300-000000-029_04_SDP_to_TM_MID_ICD and 100-000000-029_04_SDP_to_TM_LOW_ICD. [RD05]

The Delivery Component and Connector View Document SKA-TEL-SDP-0000013 shows the relationship to the SRCs and the Observatory [RD06].

2.4. Element Behavior

Not applicable

3. Context Diagram

Not applicable, this is the highest level

4. Variability Guide

Not applicable

5. Rationale

SDP interacts mostly with other systems, with little direct user interaction outside of the system, with the exception of telescope operators. We have to place some trust in these other systems being secure to avoid excessive operational overheads.

We need to invest in edge security, as SDP might become a target for attack due to being a large HPC installation with a large Wide Area Network (WAN) connection that could be used for a DOS attack against other systems with access to the WAN network

We assume that the WAN network will be engineered to so that it is only accessible from a small number of hosts worldwide to limit the its vulnerability. These hosts will included SRCs and other sites needing to access SDP Science Data Products. We also assume that the SRCs will complete appropriate security audits that would form part of an MoU with the SKA Headquarters.

We should offer some protection against non-malicious attacks, such as software bugs or human error, though currently this view focuses on external attacks.

Since some metadata and Data Products will not be publically available when it is first created, there are data access policies that should be enforced (see Quality Attribute scenario). The systems and enforcement mechanisms must be secure to achieve this.

5.1 Quality Attribute Scenarios

The following Quality Attribute Scenarios [AD03] shall be addressed in this view:

SDP_REQ-831 - Security

Scenario to be defined.

5.2.1. SDP_REQ-285 Accessibility

The SDP shall enable per user access to SDP resources (hardware and software) using the Authentication and Authorization facilities provided by the SKA.

SDP_REQ-571 Access to Science Data Products

The SDP shall allow access to Science Data Products to authorised users according to the Science Data Access policy (TBW). Authorisation will be done via SKA Authentication and Authorisation.

Scenario Refinement for Scenario 1.1		
Scenario(s)		Delivery system software must be secure and protected using SKA authorization.
Business Goals		Enforce data access policy for data products
Relevant Quality Attributes		Security
Scenario Components	Stimulus	Detection of unauthorised access to data products, intentional or unintentional.
	Stimulus Source	Human or system
	Environment	During normal operation and during maintenance, down-time, etc. Operation with the SKA data access policy.
	Artifact (If Known)	All software that can access data products. Access logs. Data product storage systems (preservation system, delivery system, SRC storage, backup storage, etc.). SKA A&A system.
	Response	Prevent further unauthorised access to data products. Determine the intent of unauthorised access. Record all access to data products. Fix the bug in the system. Inform the SKA Observatory.
	Response Measure	Once unauthorised access has occurred, prevent further unauthorised access within 1 minute until issue is resolved. Communication within one day. Fixes provided within one week. If that is not feasible then provide mitigation within one week until the fix is ready.

		Communication about fix or mitigation within one week or as soon as available.
Questions		
Issues		

6. Related Views

The security view relates to the SKA-TEL-SDP-0000013 The Delivery Component and Connector View [RD06]. Further context is provided by [RD02] SKA Regional Centre Requirements.

7. References

7.1. Applicable Documents

The following documents are applicable to the extent stated herein. In the event of conflict between the contents of the applicable documents and this document, **the applicable documents** shall take precedence.

[AD01] Shibboleth Authentication Service from Interenet2
https://www.internet2.edu/products-services/trust-identity/shibboleth/

[AD02] COmanage Authorization Service from Interenet2
https://www.internet2.edu/products-services/trust-identity/comanage/

[AD03] SDP Requirements and Compliance Statement SKA-TEL-SDP-0000033

7.2. Reference Documents

The following documents are referenced in this document. In the event of conflict between the contents of the referenced documents and this document, **this document** shall take precedence.

[RD01] SKA-TEL-SDP-0000013 Operational System Component and Connector View

[RD02] SKA-TEL-SKO-0000735, SKA Regional Centre Requirements, R. C. Bolton and the SRCCG

[RD03] SDP-CSP Interface Control Document.
300-000000-002_04_MID_SDP-CSP-ICD and
100-000000-002_04_LOW_SDP-CSP-ICD

[RD04] LFAA Interface Control Document. 100-000000-033_01_LOW

[RD05] SDP-TM Interface Control Document.
300-000000-029_04_SDP_to_TM_MID_ICD
and 100-000000-029_04_SDP_to_TM_LOW_ICD.

[RD06] SKA-TEL-SDP-0000013. The Delivery Component and Connector View

8. Version History

Version	Date of Issue	Prepared by	Comments
05	2018-04-23	R. Simmonds et al	Prepared for M20 pre-CDR delivery