SDP System-level Security View

Contributors: R. Simmonds, P. Wortmann, V. Allan

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

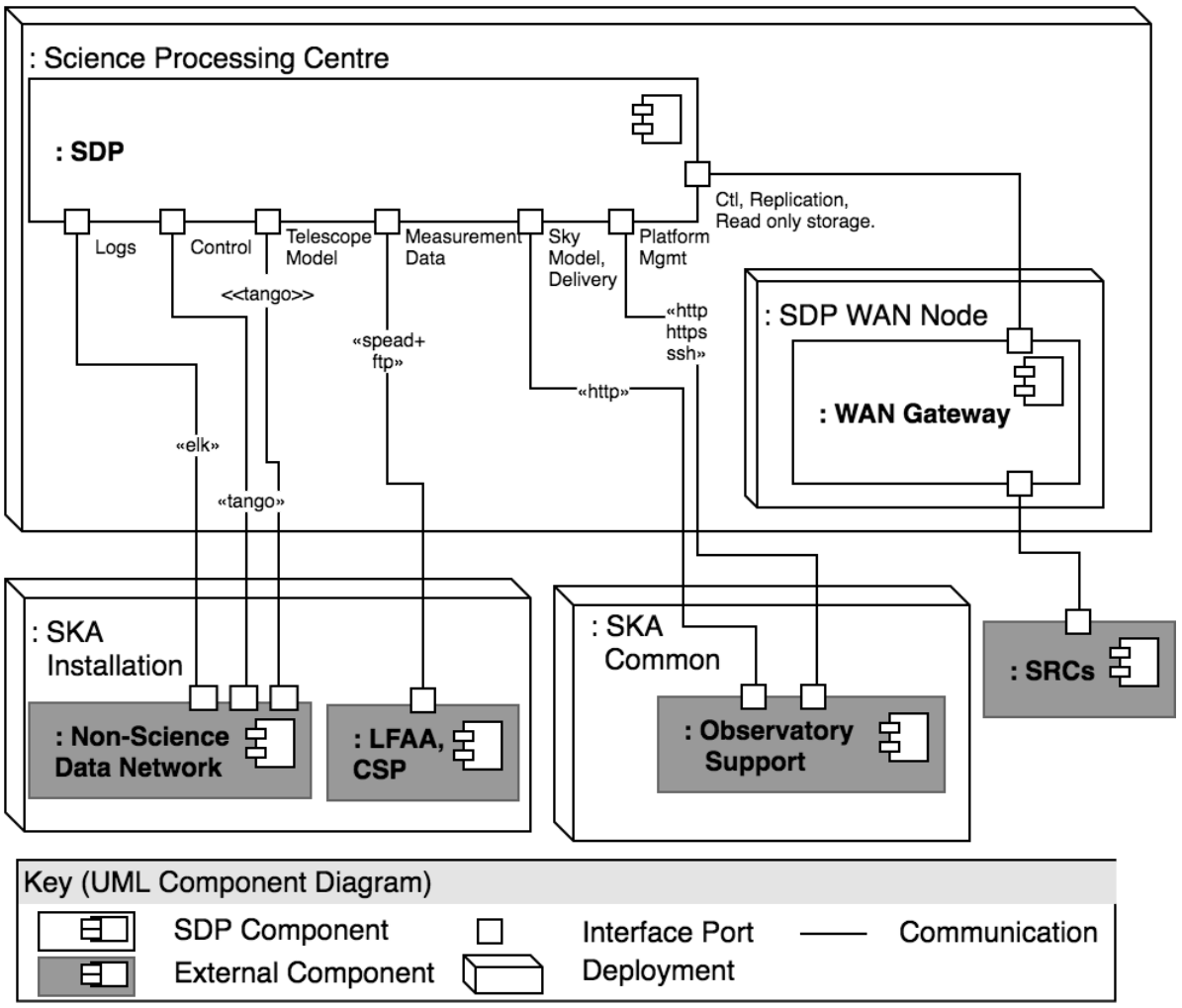

Figure 1: SDP connections to other components. SDP interaction with SRCs is performed through the SDP WAN Gateway component to isolate the high speed WAN with limited firewalling from the rest of SDP.

The Primary Representation shows the Science Processing Centre (SPC) that hosts the Science Data Processor (SDP) and the Telescope Manager (TM). There will be one SPC in each of the host countries associated with the installation site that hosts the Central Signal Processor (CSP) in that country. Each of the SDP sites also connects to SKA-Common which is software that will be deployed at the SKA Observatory 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 SKA HQ) 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. This should be protected by a Virtual Private Network (VPN) appliance provided by the hosting centre.

4. The WAN connecting to the SRCs. This is isolated from the rest of the SDP by a WAN Gateway that restricts access to internal components.

The SDP sites will exchange catalogue information through the WAN, but will not transfer data products between each other.

Note that in general Authentication Authorisation Access and Identity management (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 [AD22] deployments will be provided for authentication and role based authorisation services, such as COmanage [AD23], will be provided to service these calls.

Also note that security needs to be reviewed regularly and the SKA should conform to the security policies defined in documentation such as the NIST Cybersecurity Framework [RD01] which is updated regularly to track risks.

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 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 SPC 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 SPC local management network needs be be accessed from outside of the physical data centre, this access should be performed over a Virtual Private Network (VPN), access to which is restricted to essential operations staff.

2.1.2 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: Critical, 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.

2.1.3 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 Low Frequency Aperture Array (LFAA) and the Central Signal Processing (CSP) facility will be connected via the high speed ingest network that leads from the SKA antennae / dish Installation sites to the associated 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.

2.1.4 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.

2.1.5 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 SKAO on request. A separate security zone within the WAN Gateway will run the Regional Centre Access component via which an SRC operator who is authorised to do so, can request SDP Data Products and monitor the progress of transfers to their site.

This network also handles the replication of the Science Data Product Catalogue to the SRCs. Given that this is an engineered network with limited access the risk of the replication interfaces being compromised by an external agent is small. However, the amount of traffic generated by this is small and could be protected by an additional security layer such as an encrypted tunnel or by using ssl based connection, if this is supported by the chosen database replication implementation.

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. An Interface Definition Document is being written for the interface with the SRCs, but this is not part of the CDR submission. 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). [AD06, AD10]

LFAA: The interface to LFAA is described in 100-000000-033_01_LOW_SDP-LFAA-ICD. [AD09]

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. [AD08, AD12]

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

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.

There is a need to invest in edge security, as SDP might become a target for attack due to being a large High Performance Computing (HPC) installation with a large Wide Area Network (WAN)

connection that could be used for a Denial of Service (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 its vulnerability. These hosts will include SRCs and other sites needing to access SDP Data Products. We also assume that the SRCs will complete appropriate security audits that would form part of an MoU with the SKAO HQ.

There should also be 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 publicly available when it is first created, there will be data access policies that should be enforced (see Quality Attribute scenarios). 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:

5.1.1 SDP_REQ-831 - Security

Scenario to be defined.

5.1.2 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.

5.1.3 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.

6 Related Views

The security view relates to the SKA-TEL-SDP-0000013 The Delivery Component and Connector View. 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.
This list of applicable documents applies to the whole of the SDP Architecture.

[AD01] SKA-TEL-SKO-0000002 SKA1 System Baseline Design V2, Rev 03[1]

[AD02] SKA-TEL-SKO-0000008 SKA1 Phase 1 System Requirement Specification, Rev 11

[AD03] SKA-TEL-SDP-0000033 SDP Requirements Specification and Compliance Matrix, Rev 04

[AD04] SKA-TEL-SKO-0000307 SKA1 Operational Concept Documents, Rev 03

[AD05] 000-000000-010 SKA1 Control System Guidelines, Rev 01

[AD06] 100-000000-002 SKA1 LOW SDP to CSP ICD, Rev 06

[AD07] 100-000000-025 SKA1 LOW SDP to SaDT ICD, Rev 05

[AD08] 100-000000-029 SKA1 LOW SDP to TM ICD, Rev 05

[AD09] 100-000000-033 SKA1 LOW SDP to LFAA Interface Control Document (ICD), Rev 02

[AD10] 300-000000-002 SKA1 MID SDP to CSP ICD, Rev 06

[AD11] 300-000000-025 SKA1 MID SDP to SaDT ICD, Rev 05

[AD12] 300-000000-029 SKA1 MID SDP to TM ICD, Rev 05

[AD13] SKA-TEL-SKO-0000484 SKA1 SDP to INFRA-AUS and SKA SA Interface Control Document, Rev 02

[AD14] SKA-TEL-SKO-0000661 Fundamental SKA Software and Hardware Description Language Standards Rev 02

[AD15] http://www.ivoa.net/documents/TAP/

[AD16] http://www.ivoa.net/documents/latest/SIA.html

[AD17] http://www.ivoa.net/documents/DataLink/

[AD18] http://www.ivoa.net/documents/SSA/

[AD19] Memorandum of Understanding between the SKA organisation and National Radio Astronomy Observatory relating to a work package for the study and design of a new data model for the CASA software package

[AD20] MeasurementSet definition version 3.0. MSv3 team, eds. 2018. http://casacore.github.io/casacore-notes/264

[AD22] Shibboleth Authentication Service from Interenet2 https://www.internet2.edu/products-services/trust-identity/shibboleth/

[AD23] COmanage Authorization Service from Interenet2 https://www.internet2.edu/products-services/trust-identity/comanage/

[AD24] SKA-TEL-SKO-0000990 SKA Software Verification and Testing Plan

[1] This document is still a draft version and therefore not truly applicable, but will be replaced by an applicable version by System CDR.

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] https://www.nist.gov/cyberframework

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