Kortext stream

Est 2013

Universal Service Definition Document

Cloud-delivered Kortext stream

Version 3.0

Microsoft Azure

Document Information

Kortext stream v4	Universal Service Definition Document Kortext stream - cloud		
Prepared By:	Andrew Bates	**Version No:**	3.0
Title:	Service Definition Document (Cloud)	**Version Date:**	20/01/26
Reviewed By:	Mark Edmondson	**Review Date:**	23/01/26

Distribution Information

From	Organisation	Contact Details

To	Organisation	Date Sent	Contact Details

Ver. No.	Ver. Date	Revised By	Description	Reviewer	Status
0.01	18/06/18	REG	Initial draft	N/A	Draft
2.00	01/07/21	REG	Replacement SDD	D Winter	Issued
2.01	27/07/21	REG	RTO/RPO & WAF updates	D Winter	Issued
2.02	04/11/21	REG	Brand update	SS	Issued
3.0	23/01/26	AB	Updated to reflect current position	ME	Issued

This document version replaces all previous issues.

Restriction on disclosure

Table of Contents

Summary of tables

Table of figures

Description of services

1 Onboarding and deployment services

Every stream deployment begins with a Kortext stream Technical Enablement and Onboarding process. The approach developed by Kortext is to aggregate and translate the supplied data assets (activity files + student data) into engagement insights. Kortext stream is powered by a proprietary algorithm. This is applied without the deployment of the associated application architecture for rapid insight generation, whether for the purposes of modelling engagement characteristics for specific groups of students or the creation of insights as a technical/business proof point.

1.1 Data collection

Data collection involves the provision of data to an agreed location (such as a secure Microsoft Teams site).

1.2 Output

Data model presentation and associated PDF report.

1.2.1 Prerequisites

- Data Sharing Agreement

2 Cloud implementation services

2.1 Implementation

The customer's stream application is deployed within the Microsoft Azure cloud environment.

2.2 Authentication integration

User authentication is handled via Shibboleth, which acts as an intermediary between the Stream application and the customer's Entra ID (Azure AD) identity provider.

2.3 Hosting & monitoring services

The application is hosted within Kortext-managed infrastructure. Monitoring is performed as part of standard business-as-usual operations.

2.4 Web Application Firewall (WAF)

All traffic is routed through Azure Application Gateway with Web Application Firewall enabled, configured with OWASP rule sets to protect against common web vulnerabilities.

2.1.1 SLAs

See *Service levels*

2.2 Maintenance

2.2.1 Restore

This is only performed in response to an incident and on the request of the institution. The restore process will involve either (a) a point in time restore using database redo logs or (b) the recovery of a snapshot and then a manual backup/restore from the snapshot recovery instance. Typically, a point in time restore will be sufficient.

2.3 Penetration testing (app check)

2.3.1 Pre-build

Kortext utilises a security intelligence tool called Snyk[1], which allows Kortext to conduct vulnerability scanning at a code level to ensure we secure our code at the very start of the build process.

2.3.2 Post-build

Major versions of Kortext stream are penetration tested prior to release, and at least once a year. The relevant penetration test report can be made available on request.

2.4 Disaster recovery

All data is stored in a database configured for high availability with zone-redundant replication. In the event of a failure or during planned

[1] https://snyk.io

maintenance, failover is handled automatically by the platform to ensure continuity of service.

3 Candidate system integrations (data connectors)

To connect to the various data sources at the university stream uses micro services. These services connect to the data source and transform the data to the format required for stream, in some cases, these require minor changes for each installation of the stream solution.

Kortext stream has been designed to collate university data on scheduled basis, typically daily (overnight) after the university has completed its own daily processing of the data. This configuration will be unique for each institution as this relates to the data sources used, the data dependency on the engagement scoring and the time that the processing that it is planned to run. Specific configuration are included in project documentation and Service Desk records.

Please note: The data supplied must remain in the format prescribed in the data definition document and tested in the initial deployment and UAT. Any changes to the source data formatting will impact on the operation of stream. If a change to this data is required, this must follow the defined change request process as defined in this document. Any changes made to data formatting outside of this procedure may result in professional services charges being applied, service downtime and/or service impact.

Kortext will work with partner institutions to improve data and error capture processes to ensure the continued performance of your stream solution.

4 Analytics process (engagement scoring models)

Specific patterns were created at implementation; these can be modified for specific cohorts and groups. Any data tuning and analytics changes (e.g. additional data sources, annual model evaluation and re-calibration) will be subject to the service charges or contracted service hours.

See Onboarding and deployment services

4.1 Initial calibration

Kortext will provide a baseline model that will be agreed through the delivery of the onboarding service. This baseline model will be agreed through the implementation service or as part of your change management routines.

5 Staging and sandbox environments

A staging environment is available for testing new software releases and configuration changes prior to deployment to production.

This environment mirrors the production configuration but operates with reduced compute resources. Access is restricted to authorised customer staff only.

Issues relating to the staging environment are classified as P4 priority and will not be escalated beyond this level.

Access to an optional sandbox environment can be provided subject to commercial considerations. Details on request.

5.1 Change management

See *Change, testing & development*

6 Post-implementation support

Once the technical enablement has been completed, our specialised team will deliver ongoing support and services.

6.1.1 4-week initial 'warranty' premium support (Project Management oversight)

Kortext warrants that for a period of 28 days from the service go-live date that the software will conform to the applicable project documentation provided by Kortext in all material respects. All software errors will be corrected and remedied and managed by the Kortext PM resources. The warranty does not apply to changes in the data sources.

6.1.2 9x5x5 Service Desk

Standard service hours excluding English Bank Holidays and company closed days published in advance via the Kortext Service Desk.

6.1.3 SLAs

See *Production services*

7 Production services

7.1 3rd line support

9x5x5 Support, excluding English Bank Holidays & company closed days via the Kortext Service Desk (an analyst is always available).

See *Operational / production support*Operational / production support

7.2 Maintenance

Moves, Adds & Changes (MAC) are subject to service hours.

7.3 Software updates

Software updates, including all major and minor releases, are deployed at the provider's discretion throughout the subscription term. Customers will receive advance notification of scheduled updates.

7.4 Exit plan definition & execution

Available on request.

7.4.1 Introduction

Kortext provides support to aid exit and transition of institutional data at the conclusion of a stream service contract. This document has been created to structure exit and transition or disposal of university data processed in the stream application. This document does not cover transition or migration services to 3rd party application providers.

7.4.2 Safeguards

As an ISO 27001 certified business, all data is subject to control and treated as confidential. Kortext operate systems and processes to render data unrecoverable to prevent accidental loss or unauthorised access for any data that is not feasible for return.

7.4.3 Agreement

Within 30 days after the termination or expiration of a Purchase Order, Contract or Agreement for any reason Clause 13 of the Kortext terms and conditions will apply, Kortext shall either: return or destroy, as applicable, all sensitive data provided to Kortext by institution including all sensitive data provided to Kortext's employees; or in the event that returning or destroying the sensitive data is not feasible, provide notification of the conditions that make return or destruction not feasible, in which case, Kortext will continue to protect all sensitive data that it retains and agree to limit further uses and disclosures of such data.

The university will own all right, title and interest in and to all of the customer data and shall have sole responsibility for the legality, reliability, integrity, accuracy and quality of the customer data.

The customer will be responsible for the testing and assurance strategy relating to the data upon termination.

7.4.4 Data transition services

Any transition of data whether to a 3rd party provider or otherwise beyond the scope of the decommissioning process will be subject to a separate statement of works (SOW) with associated professional service charges.

7.4.5 Decommissioning process

Upon termination of the contract, Kortext will decommission the customer's environment from our cloud platform on a mutually agreed date.

Prior to decommissioning, customers may request an extract of their data. Once the decommissioning process is complete, all customer data is permanently deleted and is not retained by Kortext, in accordance with the terms of the contract.

8 Professional services

Included in the subscription services are hours for professional services; these are allocated based on your contracted terms and by agreement in your initial order, any remaining unused hours shall not be carried over to the next year. Hours worked are recorded and tracked via our Service Desk ticketing system. The intention of the professional services hours is to

support the change management process where there are requests that fall out of normal service support. Additional professional service hours can be procured on a case-by-case basis. This will be subject to professional services charges under a customer agreed statement of work or the Service Desk ticket.

Examples of work categories may include (non-exhaustive list):

- Ad-hoc reporting requests
- Server move support
- New connector/connector moves
- Configuration changes
- System maintenance – planned/unplanned
- System rectification from unplanned outages
- Additional customer success requirements

8.1 Customer success support

Provision of customer success support is defined by the business enablement package(s) initially purchased. All customers will receive the full standard onboarding package essential to a successful initial deployment of Kortext stream and will be supported post-onboarding by a dedicated Account Director. Additional onboarding consultancy support is available at extra charge.

Provision of additional customer success support over and above contractual allowance or repeat training sessions can be utilised as part of the customer services allowance. Any additional hours required will be quoted and agreed in statement of works or Service Desk ticket.

9 Operational / production support

9.1 Kortext stream support model

Kortext stream operate a 3rd line support model. 3rd line services will interface with your IT Operations with named contacts. End user support will be provided by university staff to its users. The university will provide the first point (1st line) of contact for support calls and will log and triage (2nd line) all calls before raising a ticket on the Kortext stream Service Desk (see Figure 1 - Kortext support model).

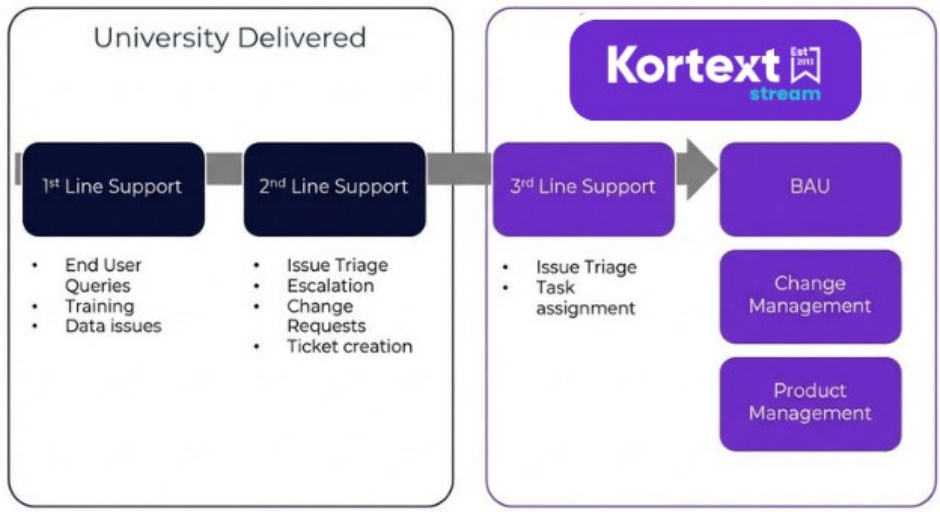

Figure 1 - Kortext support model

9.2 Service hours

All 3rd line technical support is provided 09.00-17.00hrs Monday to Friday, excluding English Bank Holidays. The Service Desk is closed between Christmas and New Year, but a Kortext stream analyst is always available should an issue arise.

TYPE	METHOD	INFORMATION SOURCE
Incident	Service Desk Portal	https://Kortext.atlassian.net/servicedesk/customer/portals
Escalations	Escalation route	Escalation routes are provided via the Service Desk
Monitoring	Service monitoring	Kortext stream Health Service Monitoring – system generated emails

Table 1 - Support Contact Details

9.3 Fair usage

Within this clause, there is a mutual fair usage undertaking that should ensure the fair usage is mutual in that Kortext cannot be responsible for service non-availability if we are not able to access the device or campus for any reason. Similarly, no SLA can be guaranteed due to any user or customer interruption; wilfully or otherwise created that prevented service availability (i.e. unplanned patching).

9.4 Post-launch project management

Following completion of the onboarding project phase, client relationships will be managed by an Account Director. During this 'business-as-usual' phase, any additional work above 5 days will be subject to a defined statement of work and agreed with the client. The work will be subject to project management processes and delivery schedules.

10 Change, testing & development

10.1 Maintenance (cloud)

Please see *Cloud implementation services*.

10.2 Changes to university infrastructure

A "Service Owner" at the university will be assigned.
The university IT Technical Team will be responsible for informing Kortext of any changes to university infrastructure outside of the scope and control of Kortext. The Service Owner should notify Kortext via the Service Desk and provide relevant details.

10.3 Standard change

A **Standard Change** is considered a change that follows an established path, is relatively common, and is the accepted solution to a specific requirement or set of requirements. The objective of this type of change is to improve efficiency and effectiveness, without creating unnecessarily high levels of administration.

A Standard Change is authorised and pre-approved, meaning that it can be carried out without seeking approval first if it meets the following criteria:

- it is a common low risk task
- procedural documentation exists for the task
- activities/tasks are well known and proven
- it is repeatable
- it is an accepted solution to a specific business requirement
- it is agreed by the line manager of the area submitting it
- it is agreed by Change Management

- it has been implemented as a Normal Change at least once prior to standardisation

10.3.1 Examples:

- Connector updates/ new connector deployments
- User Interface Configuration Updates
- Changes to resource allocation within the compute cluster

Note, this is not an exhaustive list.

10.4 Normal change

A Normal Change is a Change that is not an Emergency Change or a Standard change. Normal changes follow the defined steps of the Change Management process.
Examples:

- Software release
- Server Maintenance

10.5 Emergency change

An Emergency Change is an Unplanned System Outage or Non-Compliance - Business Critical Change, Legal Compliance Change, or Security Issue Change. It is **NOT** a Normal Change that has been submitted outside the required notice period. An emergency change would be triggered by an incident.

Due to the nature of emergency changes the timescales within which they are undertaken are usually minimal, the work itself is often implemented without full knowledge of the effects on other systems and services; therefore, it is important that the correct individuals and groups are kept informed of the plans and outcomes of any emergency changes. This can only be completed with the approval of the nominated escalation names.

10.6 Emergency routine

Should there be a requirement to undertake 'emergency' maintenance to the stream application, Kortext will provide the customer with 24 hours advance notice. Where the customer wishes to perform emergency

maintenance then the customer will provide Kortext with 24 hours advance notice.

In scenarios where an emergency negates the ability to provide 24-hour notice, contact must be made with Kortext prior to performing emergency maintenance with details. This will enable Kortext to analyse any risk or impact on the solution and schedule resource to support if needed. Without prior notification Kortext will be unable to provide short notice support.

10.7 Customer self-service management

Client issues should be triaged and addressed by the customer in the first instance. Kortext provide 3rd line support as detailed above.

10.8 Testing

Kortext operates a combination of manual and automated testing of the standard application. Localisation and the unique nature of each institution's data landscape mean that testing has limitations.

10.9 User testing

The university should provide business users (staff/student) or acceptable substitutions from the business sponsor to undertake user acceptance testing of the baseline application. This would be accomplished through support by Kortext who will provide a list of common tasks for the users to complete and measure. Post implementation, we recommend testing is conducted based on release note recommendations.

10.10 Features

The Kortext change schedule is primarily driven by a continual gap analysis of our solutions; this identifies candidates for enhancements. Customer-driven change requests should be logged via the Service Desk portal 'Suggest an improvement' option.

If a **defect** is found, an issue report is completed via the Service Desk (P4). Kortext operates a database of defects and feature requests for our solution, providing relevant updates to clients.

10.10.1 Defects

Defects are resolved at the earliest opportunity, for the purposes of distinguishing defects from feature requests:

DEFINITION	DESCRIPTION	RELEASE ROUTE
D1 (P1) Blocker	Reserved for client specific catastrophic corrupt data which (a) prevents somebody from completing an institution critical task, and (b) have no workaround. Where identified as a wider issue a hotfix may be issued to all clients as per D2.	Client Specific Hot Fix with no down time
D2 (P2) Critical	Reserved for catastrophic failures – exceptions, crashes, potential for corrupting data where specific conditions are met. These issues prevent an institution from completing significant and/or critical functions. No work around is available.	Hot Fix with no down time
D3 Major	Reserved for significant failures – exceptions, crashes, potential for corrupting data where specific conditions are met. These issues prevent an institution from completing major functions. A workaround is available. Where no workaround exists, the issue is escalated to D2 Critical and resolved via a Hot Fix.	Hot Fix with no down time
D4 Minor	Reserved for performance issues. Anything that hampers productivity but does not actually prevent work from being done.	Bug fix in next release
D5 Nuisance	These are 'nuisance' bugs. A default setting is not being applied, a non-critical read-only field showing as editable (or vice-versa), a rare condition in the UI, a misleading error message etc.	Prioritised via User Group

Table 2 - Defect priorities

All defects will be triaged to determine the correct status.

Please note that fixes will only be applied to the most recent release of the application.

10.10.2 Features/Environment Changes and Change Requests

This reflects additional requests for information where not explicitly defined with individual SLAs, and requests where service is not experiencing negative impacts.

11 Data management

11.1 Data archiving

It is the responsibility of the university to keep historical copies of the source data if required for their operations.

The stream platform will retain the data for the contract period unless otherwise directed. At times, we may need to remove certain data as part of routine operational processes. In cases where the impact is assessed as low or medium, this may occur without needing explicit approval from clients. In these situations, Kortext is not liable for any resulting data removal. Data will be subsequently re-ingested from source.

11.2 Data deletion

Data will be removed from the system upon request from the university based on criteria set by the university.

12 Prerequisites

12.1 Service prerequisites

12.1.1 Users

No users (staff or students) will have direct access to the core application and database throughout the service term.

All service users will be members of the university, excluding research staff (unless agreed in advance by Kortext) and 3rd party contractors.
All processes that require any modification directly to the backend of stream, such as config files, translation files, database tables are to be managed solely by Kortext. Where a UI built by Kortext exists to manage any of these settings, they can be managed by the university.

If the university wishes to manage something that currently does not have a UI to manage, they must submit the request as a change request to Kortext who will assess as per our change management process, where the request will get reviewed and prioritised accordingly.

12.1.2 Storage & application performance (Cloud)

Please see *Cloud implementation services*

12.2 VPN license & remote access arrangements

The university will provide VPN access and provide the appropriate security logging for audit purposes. Kortext will retain records of access to systems via Service Desk ticketing.

12.3 Additional infrastructure components

Responsibility for infrastructure is divided at the platform boundary. Kortext manages all infrastructure, networking, and security within the Kortext platform. The customer is responsible for any infrastructure, networking, and security within their own environment, including connectivity to the Kortext platform.

12.4 General

The stream software has been supplied on the understanding that the following prerequisites apply:

1. The university has supplied in an accurate form, validated source data and will be consistently provided in the same manner to allow the software to perform as designed,
2. Kortext staff will have access to university staff that have the appropriate knowledge and understanding for Kortext to perform their tasks throughout the contract term,
3. Appropriate data protection measures are in place at all times and supplied by the university throughout the duration of the contract, or while the stream software is hosted on university-managed servers.
4. No data derived from stream will be shared with any 3rd parties without consent from Kortext. Information may be shared with 3rd parties in an educational delivery partnership where it is necessary to support student progress meetings. Data can only be shared where the university is covered by a data sharing agreement and protects Kortext's intellectual property.
5. Kortext to have unobstructed UI access via institutional SSO or direct connection.

13 Assumptions and exclusions

In producing this Service Definition Document, the following applies:

1. The prerequisites as detailed in this document shall be met by the university

2. Other than data detailed in this document, all data points will remain out of scope of the stream solution and are supported and maintained by the university
3. The support service provides technical support services on the stream application and the interpretation of the analytics only.
4. Any additional costs of licenses or infrastructure not included in the solution, or 3rd party consultancy is the responsibility of the university.
5. Other than where specifically agreed all work will be carried out during normal office hours (09.00-17.00hrs Monday-Friday, excl. English Bank Holidays and company closed days, notified in advance, when an analyst will be available).

14 Additional fee structures

No work will be carried out over and above the agreed contractual payment terms without prior approval on a statement of works. All work will be scoped and costed based on the resourcing required to complete the work.

Resource fee structures are available on request.

14.1 Software warranty

An Escrow agreement is available with the current released version of the stream application. Fees apply (set up and annual service charge).

15 Service levels

15.1 Purpose and scope

The university depends on software and services (together: 'The stream solution') that are provided, maintained, and supported by the supplier. Some of these items are of critical importance to the business.

This SLA sets out what levels of availability and support the university are guaranteed to receive for specific parts of the stream solution. It also explains what penalties will be applied to the supplier should it fail to meet these levels.

This SLA forms an important part of the contract between the university and the supplier. It aims to enable the two parties to work together effectively.

15.2 Equipment, software and services covered

This SLA covers only the equipment, software and services in the table below. This list may be updated at any time, with agreement from both the university and supplier.

Please note:

- The supplier guarantees response times for all items listed in this section.
- The supplier guarantees uptime only for items with a cross in the covered for uptime column.

These items have been assigned a priority level, from 1 (most important) to 3 (least important). The priority levels help determine the guaranteed uptime and response time.

Item Type	QTY	Priority	Covered in uptime?
stream_Core Application	1	1	☒
stream_UI	1	1	☒
stream_Connectors	>10	2	☐
stream QA	1	2	☐

Table 3 - Product SLA Priority Matrix

15.3 Exclusions

This SLA is written in a spirit of partnership. The supplier will always do everything possible to rectify every issue in a timely manner. However, there are a few exclusions.

This SLA does not apply to:

- Any equipment, software, services or other parts of the stream solution not listed above
- Software, equipment or services not purchased via and managed by Kortext
- Equipment, software or services supplied by the university to Kortext in support of the stream solution
- Development or test environments of the stream solution
- 3rd party data connectors.

Additionally, this SLA does not apply when:

- The problem has been caused by using equipment, software or service(s) in a way that is not recommended.
- The university has made unauthorised changes to the configuration or set up of affected equipment, software or services.
- The university has prevented the supplier from performing required maintenance and update tasks.
- The issue has been caused by unsupported equipment, software or other services.
- Use of the stream solution in a manner that is in breach of this agreement and the contract it has with the supplier.

This SLA does not apply in circumstances that could be reasonably said to be beyond the supplier's control. For instance: floods, war, acts of god etc. This SLA also does not apply if the university is in breach of its contract with the supplier for any reason (e.g. late payment of fees).

Kortext aims to be helpful and always accommodating and will do its absolute best to assist the university wherever possible.

15.4 Responsibilities

15.4.1 Supplier responsibilities

The supplier will provide and maintain the stream solution used by the university. The IT support contract between the supplier and the university includes full details of these responsibilities.

Additionally, the supplier will:

- Ensure relevant software, services and equipment are available to the university in line with the uptime levels listed below.
- Respond to support requests within the timescales listed below.
- Take steps to escalate and resolve issues in an appropriate, timely manner.
- Maintain good communication with the university at all times.

15.4.2 University responsibilities

- The university will use the supplier-provided stream solution as intended.

- The contract between the supplier and the university includes full details of the stream solution and its intended uses.

Additionally, the university will:

- Notify the supplier of issues or problems in a timely manner.
- Provide the supplier with access to equipment, software and services for the purposes of maintenance, updates and fault prevention.
- Maintain good communication with the supplier at all times.
- Conform to the agreed service design and its dependencies without deviation during the term of the contract.
- Follow the change management processes as per the Service Definition Document.
- Provide 3rd party sponsorship/support for any data not held by the customer or data managed by a 3rd party

15.5 Guaranteed uptimes

15.5.1 Uptime levels

To enable the university to do business effectively, the supplier guarantees that certain items will be available for a certain percentage of time.

The service is delivered on a cloud-hosted, highly available architecture with defined uptime commitments. The platform targets ≥99.9% critical experience availability and is supported by resilient infrastructure, including automatic failover. Point-in-time recovery provides an RTO of 4 hours and an RPO of 5 minutes.

Availability and incident handling are governed by this Service Definition Document and outline in the table titled Response Matrix Time. Scheduled maintenance and higher-risk changes are carried out outside core service hours to minimise disruption. Continuous monitoring supports proactive issue identification.

Where availability falls below agreed levels, issues are managed through the SLA framework, structured incident management, and defined escalation routes. Remediation and corrective actions are undertaken to restore service. Any consideration of refunds or service credits is assessed on a case-by-case basis.

15.6 Guaranteed response times

When the university raises a support issue with the supplier, the supplier promises to respond in a timely fashion.

15.6.1 Response times

The response time measures how long it takes the supplier to respond to a support request raised via the supplier's online support system.
The supplier is deemed to have responded when it has replied to the university's initial request. This may be in the form of an email or telephone call, to either provide a solution or request further information.

Guaranteed response times depend on the priority of the item(s) affected and the severity of the issue. They are shown in this table:

Priority	Description	Response time	Target resolution time
P1 - Critical	The entire Product/platform/app is "down" and inaccessible.	Within two Normal Business Hours.	Four Normal Business Hours. Continuous effort after initial response and with Customer co-operation.
P2 - High	Operation of the Product, platform or app is severely degraded, or major components of the Product, platform or app are not operational and work cannot reasonably continue. Priority 2 incidents shall be reported by telephone only.	Within four Normal Business Hours.	Within two Business Days after initial response.
P3 - Medium	Certain non-essential features of the Product, platform or app are impaired while most major components of the Product, platform or app remain functional.	Within 12 Normal Business Hours.	Within seven Business Days after initial response.
P4 - Low	Errors that are, non-disabling or cosmetic and clearly have little or no impact on the normal operation of the Product, platform or app.	Within 24 Normal Business Hours.	Next release of Software.

Table 4 - Response Time Matrix

Response times are measured from the moment the university submits a support request via the agreed support process in this Service Definition Document. SLA's will be paused when the status is 'with customer'.

Response times apply during standard working hours (9.00am — 5.00pm, Mon-Friday, excluding English Bank Holidays) only, unless the contract between the university and supplier specifically includes provisions for out of hours support.

15.7 Resolution times

The supplier will always endeavour to resolve problems as swiftly as possible. It recognises that the university's computer systems are key to its business and that any downtime can cost money and reputation.
The supplier may not be able to provide guaranteed resolution times. In all cases, the supplier will make its best efforts to resolve problems as quickly as possible. It will also provide frequent progress reports to the university.

15.8 Cloud SLA

Characteristic	L1	L2	L3
Impact of unavailability (scope)	University-wide	Faculty / Service	Team / individual
Typical number of users	1000s	100s	10s or fewer
Availability	99.9%	99.5%	99%
Redundancy approach	Highly resilient Azure across Availability Zones (UK - London) – no geographic failover		
(high-level)			
Performance	Highest		
Storage tier	N/A		

Table 5 - Cloud Services SLA Matrix

16 Architecture

The latest architecture diagrams will be provided to clients on request.

16.1 Kortext stream SSO Handling

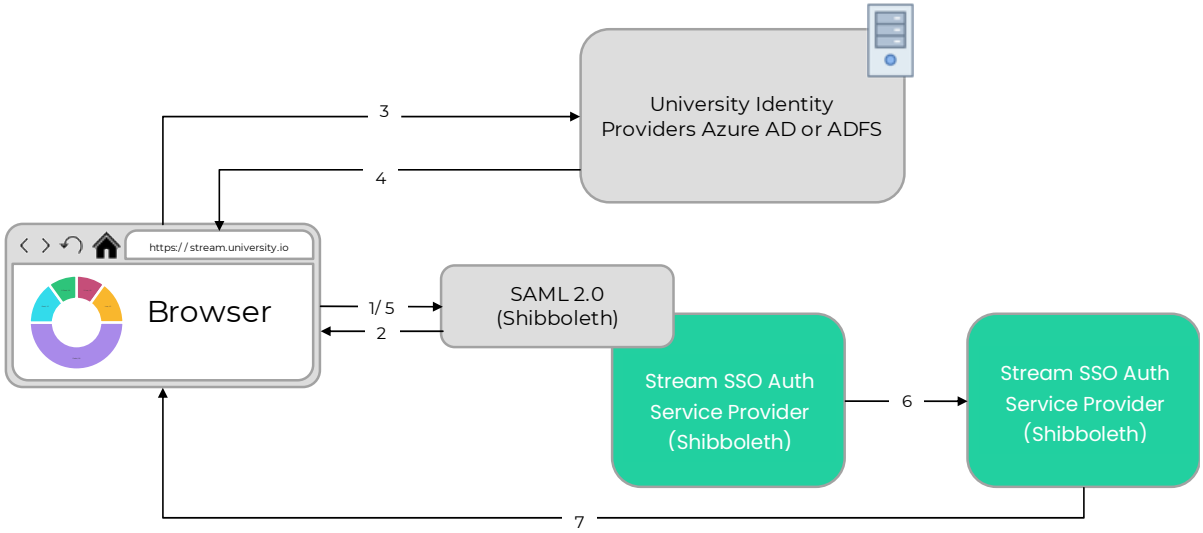

Figure 2 - SSO Handling