SAP Authentication 365
Supplemental Terms and Conditions

SAP and Customer have entered into an agreement for a subscription to certain SAP products and services ("**Agreement**") pursuant to which Customer is subscribing to SAP Authentication 365 (the "**Cloud Service**"). These Supplemental Terms and Conditions ("**Supplement**") and any modifications to the Agreement made herein apply solely to the Cloud Service and not to any other SAP product or service.

1. CLOUD SERVICE

1.1. The Cloud Service (i) generates and provides to the Customer via an API call a two-factor authentication token ("Token") in response to a request for such a Token from the Customer via an API call to the SAP network and (ii) authenticates the Token entered by the Customer's end user in the applicable Customer application after the SAP network's receipt via an API call from the Customer of such entered Token. A Token is a combination of numeric and alphanumeric characters configurable by Customer (e.g., PIN codes, verification codes, one-time password).

1.2. The Cloud Service is provided through customized API calls between Customer and SAP, along with a hosted User Interface (UI) which may be used to set defaults and view analytics and metrics. The Cloud Service may only be used by Authorized Users. The UI can be accessed by Authorized Users who are developers granted access by Customer's administrative user.

1.3. The Cloud Service **DOES NOT** include the physical transmission of a Token to a Customer's end-users ("Token-End User Transmission Service"). Subject to technical conditions that might exist within a Customer's network ecosystem, the Cloud Service is functionally compatible with multiple communications messaging technologies that can function as a Token-End User Transmission Service, including SMS text, Internet push, and e-mail transmission. CUSTOMER IS RESPONSIBLE FOR OBTAINING TOKEN-END USER TRANSMISSION SERVICE FROM A SERVICE PROVIDER OF CUSTOMER'S CHOICE. SAP CAN PROVIDE TO CUSTOMER TOKEN-END USER TRANSMISSION SERVICE IF CUSTOMER ELECTS TO RECEIVE SUCH SERVICE FROM SAP SUBJECT TO SAP'S SEPARATE APPLICABLE TOKEN-END USER TRANSMISSION SERVICE TECHNOLOGY AND SEPARATE TERMS AND CONDITIONS.

2. FEES. The Usage Metric for the Cloud Service as to which the applicable fees shall apply is the number of Successful Authentications per month. A "Successful Authentication" occurs when Customer's end user requests that the Token received on the end user's mobile device via the Token-End User Transmission Service be authenticated, and a match, meaning an "authentication," of the Token input by the end-user into the Customer's reference website or application is made by the Cloud Service with the Token generated by the Cloud Service for that end-user.

3. ADDITIONAL TERMS

3.1 Support. Support services for the Cloud Service are set forth in **Attachment 1** to this Supplement. SAP may update the support services from time to time, subject to the Continuous Modification terms of the GTC.

3.2 Cloud Service Data. Data used or generated in connection with the Cloud Service shall include the Token, the mobile directory number of the Customer's end user ("MDN"), the Token value parameters received by SAP from Customer to generate a Token with respect to a Customer request therefor, and related meta-data generated by the Cloud Service on the SAP network (collectively, "Cloud Service Data"). As between the Customer and SAP, Cloud Service Data shall be the property of SAP, including any intellectual property rights therein but excluding any MDN except for the right set forth below to retain and store all MDNs on the SAP network. SAP shall have the right, but not the obligation, to retain and store Cloud Service Data in the SAP network during term, and after the expiration or termination, of the Cloud Service. Notwithstanding the foregoing, SAP shall make available to Customer

certain of the Cloud Service Data during the term of the Cloud Service, provided that (i) each Token shall be deleted upon authentication or expiration thereof and (ii) upon expiration or termination of the Cloud Service, Customer will have no access to the Cloud Service and accordingly no access to Cloud Service Data resident on the SAP network.

Attachment 1
To
SAP Authentication 365
Supplemental Terms and Conditions
Support Services for SAP Authentication 365

This document ("Support Cloud Services Document") describes the support services provided by SAP for SAP Authentication 365.
Customer may report a suspected fault to SAP by sending an email to: 'EMSupport.sapmobileservices@sap.com' or such other email address as SAP notifies to the Customer from time to time.

To diagnose and resolve suspected faults, SAP will require certain information when the problem is first reported with as much detail as possible. This will include:

- The Hub Account(s) and/or SAP Authentication 365 account affected
- MSDISN(s) affected and / Or OrderId(s) affected

Impact (e.g. High 100% of traffic affected, Medium 20% of traffic affected, Low 1 message or administration request) "Traffic Affected" means responsiveness of the Cloud Service (e.g. API calls are not being processed or not responding, as measured in mSecs).

- Description of the problem(s)
- Company name
- Name and contact telephone number of the person reporting the fault

The Customer will ensure that the ticket number generated by SAP in response to the report of a suspected fault is included in the 'subject' field of all future correspondence in relation to such suspected fault.

Severity levels

Faults reported by the Customer will be allocated a severity level in accordance with the severity of the problem:

S1 - Severity one	A *severity one (S1)* problem consists of a fault which renders the Cloud Service unavailable. This applies to a total outage of the Cloud Service where tokens cannot be generated or authenticated.
S2 - Severity two	A *severity two (S2)* problem consists of a fault causing acute operational problems (e.g. considerable service restriction like the numerous operational API errors that are not related to implementation).
S3 - Severity three	A *severity three (S3)* problem consists of a fault which causes non--acute operational problem (e.g. delays in generating tokens or token authentication response delayed).
S4 - Severity four	A *severity four (S4)* problem consists of a fault causing the SAP Authentication 365 analytics to be partially inaccurate.

Fault Response

SAP shall endeavour to inform the Customer concerning any reproducible fault reported, to prepare an action plan and to fix any reproducible fault within the following estimated time frames:

Stage \ Severity	S1	S2	S3	S4
Initial response time	1 hour	2 hours	24 hours	48 hours
Target Restoration (work around)	2 hours	5 hours	2 working days	Reasonable time
Target Resolution	2 working days	5 working days	Next release	Next release

Initial Response Time means the target time to notify the Customer of a fault once it becomes known to SAP or to respond to the Customer's notification to SAP of a fault.

Target Restoration means the target time to find a temporary workaround for the reported fault. A temporary workaround is a solution which substantially restores Cloud Service, although some problems may persist. SAP offers no assurance that a workaround for a reported fault will be available by such target time.

Target Resolution means the target time to attain a fully restored Cloud Service.

Escalation procedure

In the event the solution detailed in the action plan are not implemented in accordance with the estimated time as set out in the preceding paragraph, SAP will apply the following escalation procedure:

In the case of S1 faults, exceeding any of (1) Initial Response, (2) Target Restoration, (3) Target Resolution times shall be reported to SAP Mobile Services' SVP Engineering. Where a S1 fault has been escalated, the parties will formulate a new, or revise an existing, action plan with additional technical and human resources to address the issue. SAP shall update the Customer on a periodic basis.

S2, S3 and faults, for which a solution is not provided within the estimated time frame and for which the same level of urgency persists, are escalated one level in classification of seriousness: S3 to S2, S2 to S1. The parties shall discuss a new, or revise an existing, action plan with additional technical and human resources to address the issue.