VeriDas

Why an integration review?
The below list comes from the experience of VERIDAS helping customers with multiple and diverse integration processes; it summarizes general recommendations/improvements, mandatory checks and several weak points an integration may have, so we strongly suggest paying special attention to them before moving forward as not doing so might cause issues in production. Please note that this might not cover every aspect in your integration, it's continuously reviewed with each new integration process and the feedback our customers provide. Please, send this document filled back to VERIDAS to help in a joint review meeting. Also, feel free to let us know your experience with this checklist. VERIDAS cannot deliver the production credentials to our customers without the approval of this checklist. VERIDAS will not, at any event, be responsible for the interpretation of the results arising from the pentest performed by the CLIENT; the CLIENT retains the final decision on the evaluation of the risks evidenced in order to decide if they can be assumed. However, and taking into consideration the risks evidenced by an eventual vulnerability, VERIDAS may demand its correction within a maximum period and, if it is not corrected, it may imply the suspension of the services for security reasons. In any case, VERIDAS discourages the entrance into production of systems which do not guarantee the information security and the protection of personal data.

Context	
Date of review	*dd month yyyy*
Customer	*Name of the company*
Integrator(s)	*Name of the company integrating the solution (if any)*
End customer	*Name of the company (if any)*
Use case	*i.e: authentication for authorzing operations, login, facial comparision against government database.....*
Authentication type	*i.e: first/second factor*
Applicable regulations	*if any*
SDK version	*i.e: HTML Selfie v3.4.8 ...*
End user platform	*i.e: React, webviews....*

Participants	
Veridas	*CS representative name*
	Sales representative name

Customer	*Name, company*

Summary
To be filled by Veridas

M	Mandatory
R	Recommended

Example evidences
screenshot, video recording, cloud/product logs, email from customer or just a comment

Checklist

Category	#	Subject	Platform	Check	R/M	Answer	Reason
Customer application	1	Flow configuration	ALL	The validation process is the expected one described in the "Corresponding validation process" in "Context" Section of this review document.	M	YES/NO	
Customer application	2	User identification	ALL	Before starting the process, the end user is identified in order to perform the authentication against the registered credential	M	YES/NO	
Customer application	3	User identification	ALL	Before starting the process, an end user anonymous id is generated.	R	YES/NO	
Customer application	4	Security measures	ALL	Measures to avoid automated attacks exists (captchas, tokenized URLs, authenticated session, contact validation (point 2))	R	YES/NO	
Customer application	5	Security measures	ALL	There is an authentication between the front side application and the middleware (recommended not to be a fix secret).	R	YES/NO	
Customer application	6	Security measures	ALL	The credentials to connect with VeriSaaS are stored in the back (milddeware), not in the front side application.	R	YES/NO	
Customer application	6	Clear instructions of the proces	ALL	Before starting the process, the user is provided with clear instructions of the steps to complete, if applicable to the use case.	R	YES/NO	
Customer application	7	Browsers compatibility	HTML	In case of a process with HTML SDKs, the user is provided with clear instructions and the list of compatible browsers (if applicable)	R	YES/NO	
Customer application	8	Non happy path processes	ALL	There is a limitted number of capture attempts in case of error or low scores. (linked with checks 1 and 2 of "Customer application" category)	R	YES/NO	
Customer application	9	Non happy path processes	ALL	If VeriSaaS returns an 5xx error, the middleware is retrying again after a few seconds.	R	YES/NO	
Customer application	10	Non happy path processes	ALL	There is an alternative authentication factor in case biometry fails or provides low scores after the limmited number of attemps.	R	YES/NO	
SDKs	1	Latest versions of SDKs.	ALL	In order to have the best user experience, best capture process and latest security fixes, the latest versions of the SDKs are being used (check our SDK documentation).	M	YES/NO	
SDKs	2	Selfie Alive Pro	ALL	Every time a user has to repeat the Selfie Alive Process process, a new challenge is requested to our API and used in the SDK.	M	YES/NO	
SDKs	3	Non happy Patth: Selfie Alive Pro	ALL	There is a limited number of attempts to complete Selfie Alive Pro challenge in the customer application/web (front)	R	YES/NO	
SDKs	4	Full screen	ALL	Veridas SDKs are being setup in full screen	R	YES/NO	
Back & API	1	Right model (if credential is used)	ALL	If credential is used, the model is provided. (no deprecated endpoint is used)	R	YES/NO	
Back & API	2	Right orchestration order	ALL	The available image is compared against the registered credential or image (Passive authentication)	M	YES/NO	
Back & API	3	Right orchestration order	ALL	The challenge is requested to the API, the score returned is validated and as a last step, the biometry authentication is performed to authenticate the user (Active authentication.), if applicable to the use case.	M	YES/NO	
Back & API	4	Sequential PUTs	ALL	PUT requests from the same authentication process need to be sent sequentially, cannot be overlapped.	M	YES/NO	
Back & API	5	Use contextual data (rtag)	ALL	The rtag parameter is being used to send relevant additional information required for billing, statistical or troubleshooting purposes.	R	YES/NO	
Back & API	6	Unnecessary API calls	ALL	No duplicate or unnecessary calls are being requested to Veridas API	R	YES/NO	
Back & API	7	Time out error (Error 499)	ALL	The timeout setup is higher than the 60 secs timeout of Veridas API.	R	YES/NO	
Back & API	8	OperationMode	ALL	The correct OperationMode (selfie or document mode) is sent to the API in order to perform the verification process between both images (full details can be found here).	R	YES/NO	
Business	1	Business rules to accept or reject	ALL	Describe which are the business rules you have set in order to accept (list scores, thresholds and other checks)	R	YES/NO	

Comments
To be filled by Customer