



# How to Choose the Right 3D Secure Software - An Issuer's Guide

Critical elements to focus on while choosing  
3D Secure software for your bank



# SUMMARY

- 1.** Assess your need for modularity of the solution
- 2.** User-friendly administration portal as a must
- 3.** Look for flexible API interface (ACS and 3DSS)
- 4.** Choose ACS user interface with local/multiple language support
- 5.** Apply customer-centric approach through ACS API
- 6.** Opt for local country and language support
- 7.** Look for omnichannel 24/7 HelpDesk service
- 8.** Assure that know-how and best practices are included



asee

With **3D Secure** you can protect your business and clients, **reduce fraud** on the merchant side, **grow your client base** and do business **without challenges** other banks face.

# Introduction

Nowadays, issuing banks face many 3D Secure technology vendors. Although it is a standardized solution, there are still significant differentiators that separate vendors that are a satisfactory fit from the ones that are an excellent fit for your business.

To aid you in your decision-making process, we prepared a comprehensive eBook covering all the critical elements you need to consider while making intelligent, well-informed decisions regarding implementing 3D Secure technology. Following those steps, you will be able to protect your business and your clients, reduce fraud on the merchant side, grow your client base and do business without challenges other banks face that passed to choose the right solution for them.

## TriDES2

**History:** 3D Secure protocol was introduced in 2001 by VISA to provide an additional security layer for card-not-present transactions. Since then, both technology and trends in the online sphere have changed drastically, demanding more flexibility, and inevitably, more security.



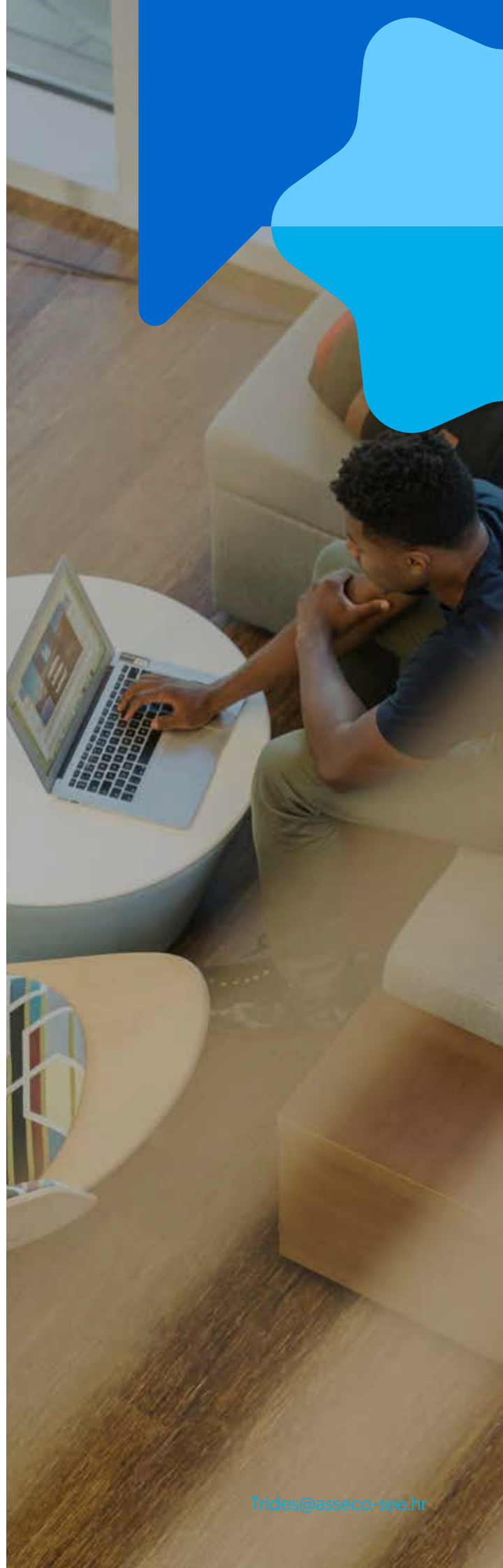
# 1. Assess your need for modularity of the solution

By overlooking the solution's modular architecture, you risk a complex and costly integration with third-party applications using standardized protocols. The main premise behind the modularity of the solution is achieving high availability according to industry-recommended and industry-accepted configurations. Without modular architecture, it can't be executed as easily.

**ACS** and **3DS** server ensure proper transaction flow and message formats, while **transaction risk scoring** and **cardholder authentication** can be organized as separate services.

When ACS relies on external services to carry out the authentication part, you can use one authentication service across all digital channels. **Modular architecture enables you to ensure superior UX for your clients.** Having uniform authentication methods and tokens across all digital channels will lead you to a more straightforward user and credential/token management.

You could apply a similar solution to risk scoring services. Solutions in which risk scoring is integrated within ACS core indeed have easier implementation and fewer integrations and connections between modules and services. The problem for you? Such risk scoring services can only score eCommerce transactions. Only a centralized risk scoring service integrated with ACS is able to provide you with such comprehensive risk analysis.



## 2.

## User-friendly administration portal as a must

3DS demands continuous monitoring of transactions, percentage of (un)successfully authenticated transactions, reasons behind declined transactions, and transaction abandonment rates from the issuing banks.

To make well-informed decisions when it comes to fitting targeted business strategy, you should have these criteria clearly presented through ACS monitoring dashboards, including visible critical parameters that enable different business owners in your bank. **It is important that you are able to track the transactions and have a birds-eye view of the overall performance at a glance.** On the other hand, in order to make 3DS business changes, you need to be able to update crucial parameters via a simple administration portal, conduct tests, and finally, release the solution into production.

**Without such dashboards, tracking vital metrics will require much more effort and lead to a potential increase in total costs** when it comes to analysis and reconfiguration of the parameters.

### 3. Look for flexible API interface (ACS and 3DSS)

The ACS solution designed as an ACS core along with satellite services enables flexibility of the solution in a way that services can be cloned, adopted to the integration point, and addressed in the ACS core configuration.

This enables you to define fine parameters, e.g., **one card** range will use **one authentication service**, while another card range will use a different authentication service. Moreover, if the authentication method is enabled, the cardholder is able to choose and switch between different authentication services, making the solution **flexible and user-friendly**.

Such ACS architecture enables advanced features for the cardholder, providing the cardholder with an option to enroll **independent authentication services** as a trusted service for 3D Secure.

#### 4.

## Choose ACS user interface with local/multiple language support

In the Payment Card Industry, standard practice is that the country of issuance defines the language at the Point of Sale. Nowadays, online shoppers are used to purchasing from foreign eCommerce stores. Still, during 3D Secure authentication, the issuing bank usually presents ACS screens in a language corresponding to the country of origin. Keeping in mind that payment cards can easily be issued to non-citizens, their user experience would be much better if the **authentication screen** offers the option to finalize the purchase in their **native language**.

The default language is a standard feature, but some **ACs provide multiple language support**. Cardholders can either set their desired language preference through mobile wallet, m-banking application, m-token application, or during the transaction taking place at the time of the initial ACS screen.

## 5. Apply customer-centric approach through ACS API

It is well known that Low-Value Payments are transactions amounting up to 30 EUR, and the issuer can allow such **transactions to be processed without demanding SCA**. Merchants are also able to request their SCA exemption which, if following MC and VISA suggestions, can be accepted by the issuer. But how can we be confident that the cardholder agrees with such decisions?

The end-users, i.e., cardholders, want to have power over their data. In other words, they want to feel as if they are the center of their service providers. **Businesses need to make sure that their service portfolio is not only broad enough so that the customer can easily decide upon their service.**

The solution to this problem lies in the customer-centric approach. You are **enabling the cardholders to manage their user experience by providing enough authentication parameters, risk scoring parameters, and other parameters related to transaction flow**. In this way, the cardholders can define whether they want to process LVP frictionless transactions, accept merchant exemption, manage Merchant Whitelist [allowing frictionless transactions] and Blacklist [demanding SCA], setup preferred [default] authentication method, language support, as well as take a look at their transaction history, etc. This puts a relief on your customer service support and enables your cardholders to tailor their user experience according to their specific needs.





## 6. Opt for local country and language support

The remote model of support has its challenges that could potentially jeopardize the overall quality of the solution. Namely, those challenges are time gaps, language, and most notably, confidentiality with local business models and trends.

**Having a local partner who is skillful enough to support first and second-level support grants you the highest possible level of support for the end-user.**

When choosing a 3D Secure technology vendor with **local country** and **language support**, make sure that local partners went through the necessary training, confirmed with relevant certificates, in order to provide support for each level of local support you need, as well as for each product and service.

## 7. Look for Omnichannel 24/7 help-desk service

3D Secure is not something that the end-user asked for. Most of them were not aware, and still aren't, about the necessity for an additional layer of security in online payments. Any inconvenience caused by the particular service, whether it concerns authentication, slow response time, sketchy authentication screens, confusing User Experience, will trigger user complaints and overwhelm your HelpDesk with inquiries. Also, the problem might occur on the merchant side, reflecting poorly on users' experience with 3D Secure. No matter the root of the problem, the end-user will most likely contact you as their bank to discuss the inconvenience.

In order to manage and solve disputes efficiently, your HelpDesk must have access to 3DS and possess the necessary knowledge regarding the 3DS process and user solution. Disputes and claims that are more complex need to be addressed by the software vendor. To ensure the **highest level of service quality, fast problem solving, and minimal delay** in resolving disputes, the Software vendor's HelpDesk service must provide you with **24/7 availability** along with **well-informed** and **skilled personnel** able to act promptly.



## 8.

## Assure that know-how and best practices are included

When the system is up and running, the onboarding of the financial institution displays the actual challenge. The issue lies in a broad set of parameters and rules regarding the transactions that must be set. The particular challenge is setting up the risk scoring rules accordingly in order to achieve targeted performance and business results.

When the institution is onboarded and all of the parameters are set in place, vendors should provide test cases to confirm the functionality of the solution and expected use cases. However, such testing provides only information about whether the setup is correct and reacts accordingly to separate use cases.

Keep in mind that the final result and impact on the business are visible after a certain period when statistical analysis can be performed. Upon analyzing those initial results, banks will need to reconfigure specific parameters in a few iterations in order to finally reach the targeted business results.

**Experienced 3D Secure SW vendors are able to provide additional value because of know-how and past experiences, helping you in reducing those iterations.** Take into consideration that parameters may vary depending on the region, bank's business strategy, the profile of end clients, local online services and its adoption to 3D Secure, PSD2 requirements, as well as the regulation of national banks and applied card schemes.

# ASEE Group as your 3D Secure partner

With over 20 years of experience in authentication, payments, risk and compliance solutions, we understand your needs. Stacked with valuable know-how and skilled professionals in industries such as banking, payments and finance, we are a resourceful partner to your company. Payten, part of the ASEE Group, provides complete payment industry solutions for financial and non-financial institutions, as well as offering support for card and cardless transactions.

In case you have any questions regarding your 3D Secure journey, we are happy to advise you and provide support along the way. To better understand what to expect from 3D Secure 2.0, we are more than happy to showcase all the functionalities of the solution using our 3DS2 DEMO platform.

## ASEE GROUP FACTS & FIGURES:

- **Top player for banking and payment industry**
- **Serving customers on 4 continents, 20+ countries**
- **190+ Banks in client network**
- **End-to-end Product/Solution portfolio for banking operations**
- **Processes +1B eCommerce transactions in a year**
- **Processes +5.5M tokenization transactions per month**

For more information, please contact us at [trides@asseco-see.hr](mailto:trides@asseco-see.hr), and arrange your free, zero-obligation consultation with our team of experts.