TriDES2 by Asseco

New generation of 3D Secure solution

3DSecure.asseco.com

asseco

Payten

MEMBER OF asseco

TriDES2 is a complete 3D secure solution for issuing and acquiring institutions who want to reduce the risk of fraudulent online payment transactions with the Strong Customer Authentication. Following the new EMV® 3-D Secure Protocol, TriDES2 enables enhanced authentication methods including Biometry, Transaction Risk Analysis and Risk-Based Authentication which improves end-user online payment experience and transaction security.

Modern day consumers have more ways to pay than ever before. E-commerce popularity has increased constantly over the last couple of years, whether through a web browser, mobile app, or a connected device. It has become an efficient and effective way for people to shop in the comfort of their own homes.

Increased number and volume of online payment transactions causes an increase in the fraudulent use of payment cards thus generating additional fraudulent and chargeback costs. Cardholders demand the most convenient user experience in online shopping environments without sacrificing high payment security standards. As the answer to all those demands, Asseco has developed the TriDES2 secure solution.

The TriDES2 solution makes online transactions more secure while significantly improving the user experience by decreasing transaction friction and by increasing the seamlessness of the authentication experience. TriDES2 development is backed up not only by years of experience and in-depth knowledge in card and mobile payment industry, but also by our expertise in authentication and security fields.

Regulatory and standards compliance

TriDES2 solution is certified in accordance with the EMV® 3-D Secure Protocol and confirmed to the PCI DSS, PCI 3DS Core Security Standard and GDPR regulations. This simplified solution implementation and compliance audits, reduce time to market and optimize your implementation costs.

TriDES2 brings benefits to whole payment chain

Cardholder

- Increased confidence in online payment when purchasing on the web or by mobile applications
- Easy to use – simple and intuitive, frictionless process and refined user experience
- Own control of payment risk parameters
- Uniformed two factor strong customer authentication and user experience across all digital channels

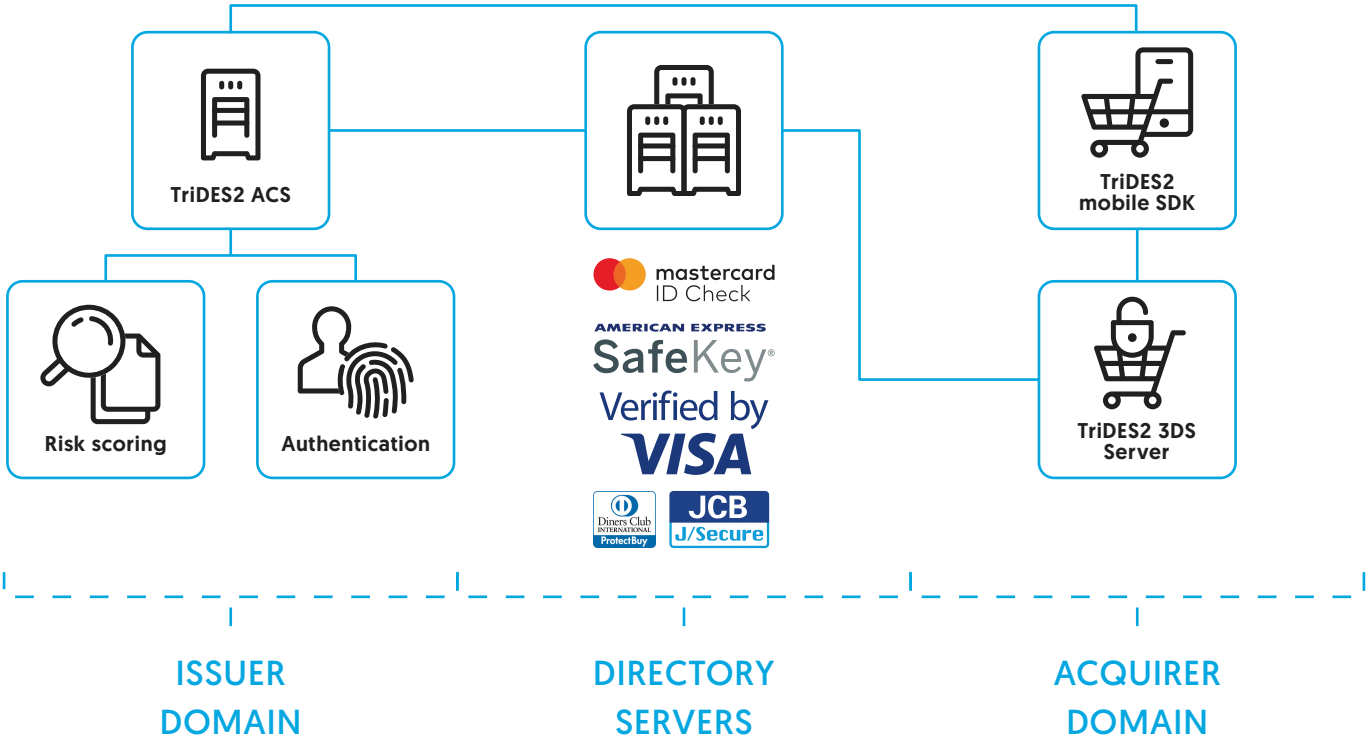
Merchants and acquirers

- Increase of sales
- Granted liability shift for fraud and disputed transactions
- Fast and easy integration
- Progressive security
- High conversion rate

Issuers

- More value to existing product offerings
- Decrease in online card fraud and disputed transactions
- Deep risk assessment of online merchants, clients and transactions
- Progressive security

TriDES2 is a complete 3D solution package



Access Control Server enables issuing institution to participate in 3D secure program by ensuring that cardholder is authenticated during online CNP transaction either through Risk based authentication or using other available authentication methods such as One time Password, SMS OTP, mobile token, biometric etc.

Based on transaction data provided by 3DSS and ACS, Risk scoring engine will evaluate transaction risk. Based on evaluated risk, online CNP transaction will be either frictionless or authenticated using available SCA method.

3DS Server enables acquiring institutions to provide 3D Secure protection to its merchants. Simple integration with web shop or mobile application, merchants will grant card scheme liability shift in case of online fraud.

In order to enable mobile purchasing applications to support 3D Secure program, mobile application vendors can use certified 3D Secure SDK. The SDK communicates with 3DSS to check if BIN is enrolled in 3D Secure, and with issuing bank ACS to ensure risk evaluation and cardholder authentication.

Key references

- Abanka Slovenia
- Addiko Bank Group (Croatia, BiH, Serbia, Montenegro)
- Bankart Slovenia
- BKT Albania
- Centre Monetique Interbancaire
- Delavska Hranilnica
- Diners Card International
- NLB Group (Prishtina, Belgrade, Sarajevo)
- Halkbank Serbia
- Hrvatska Poštanska Banka
- Mercury Processing Service International
- Nova Kreditna Bank Maribor
- OTP bank
- Privredna Banka Zagreb, Member of Intesa SanPaolo Group
- Raiffeisen Bank Austria
- SKB Slovenia, Member of Societe Generale Group
- Slovenska Sporitelna, Member of Erste Group
- Sparkasse Slovenia
- Unicredit Slovenia
- Zagrebačka banka, Member of UniCredit Group

Highlights

- Certified for supporting multiple 3D Secure card programs: Verified by Visa, Mastercard® Identity Check™, American Express Safekey®, Diners Club ProtectBuy®, JCB J/Secure™, UnionPay UPOP, NSPK MirAccept.
- Multitenancy – multiple financial institutions can be deployed at the same server instance, ensuring full data security and confidentiality along each institution.
- Highly modular architecture allowing financial institution to optimize overall solution to its need and internal infrastructure environment.
- Scalable and high availability architecture needed for 24/7/365 working mode.
- Simple and easy integration - integrability with existing on site systems (cardholder database, authentication platform, fraud management, Internet and mobile banking platforms).
- Fully aligned with PCI DSS, PCI 3DS and GDPR requirements enabling easy certification at client premise.
- Supported variety of authentication methods (One Time Password, OTP by SMS/push, QR code, Biometry, Risk Based Authentication, Out Of Band Authentication).
- Simultaneous usage of multiple authentication methods (primary and fallback methods, risk based authentication).
- Web based administration GUI built through web service enables integration with internal banking administration service.
- Platform flexibility – Java technology provides support for multiple platforms and operating systems.
- Supported different HSM devices.
- Flexible configuration of transaction flows and functionalities based on BIN, BIN range, financial institution, service provider, merchant or cardholder level.

Verified by VISA · mastercard ID Check · AMERICAN EXPRESS SafeKey · Diners Club INTERNATIONAL ProtectBuy · JCB J/Secure · UnionPay 银联

3DSecure.asseco.com

TriDES2 ACS by Asseco SEE

Security perfectly tailored to the users' need

Balancing Security and User experience

Payment security and fraud reduction are key objectives when it comes to online payments. In pursuance of these goals, PSD2 and 3D Secure 2.0 have introduced Strong Customer Authentication (SCA) as a requirement for the online card-not-present transactions, thus enabling Issuers to reduce chargeback disputes and related operating expenses.

With the objective of providing convenient end-user experience and reducing user friction in online payments, 3D Secure 2.0 is aligned with PSD2 in terms of allowing SCA exemptions, based on Transaction Risk Analysis and Risk Based Authentication.

Optimized approach

TriDES2 ACS allows issuing institutions to ensure the best user experience for their users by using frictionless Risk Based Authentication and to improve payment security through Strong Customer Authentication by means of different types of authentication methods (Biometry, OTP, C/R, MAC, QR code, ORP by SMS/Push) when shopping in a web or mobile app.

In order to deliver Risk Based Authentication and to prevent unnecessary cardholder interaction, special attention is given to the transaction risk evaluation solution. The built-in InACT Euler® fraud management solution utilizes self-learning mechanisms and enhanced econometric statistical methods to identify behavioral deviations of cardholders and to apply an appropriate authentication method.

Key Product Features

- **Multitenancy** – multiple issuing institutions and their subsidiaries can be hosted on a single TriDES2 ACS instance.
- **Modular architecture** – Components are modular and technology agnostic, so they can be implemented separately as well as integrated with third party components. Available either through integration per module or as a complete turnkey solution with built-in authentication (Asseco SEE SxS) and Risk Assessment Service (InACT Euler Enterprise Fraud Prevention and Monitoring).
- **Web based administration** with supported single sign-on for issuer administrators with simple and intuitive ACS administration and Help Desk user interface.
- **Scalable solution** – Enables optimal configuration in respect of the estimated transaction load.
- **Configurability** – allows configuration of transaction flows and functionalities on the BIN, BIN range, financial institution, service provider, or cardholder level.
- **Multiple authentication methods** – One Time Password, OTP by SMS/push, QR code, Biometry, Out Of Band Authentication, Risk Based Authentication.
- **Platform independency** – J2EE and the web service technology with XML/SOAP API enable simple and easy integration with the existing on-site systems.

Product Components

Core Module

- Processing transaction flows in conformity with the EMV® 3-D Secure Protocol, including the communication among the Issuer, directory server, and merchant domain
- BIN life cycle management

Administration

- Simple web GUI for administration
- Environment property configuration (key management, authentication types, certificate management)
- Authentication service management
- Administrator management

Tokenization

- Additional security level achieved by using a tokenized PAN within 3D Secure programs
- Asseco Tokenization service
- Integration with external third party tokenization services

Authentication

- Integration with multiple Asseco's or third party authentication solutions
- Configuration of primary and secondary authentication methods on the BIN, BIN range, issuing institution or cardholder level.

HSM Interface

- Integration with multiple and different types of HSMs

Reporting

- Built-in extensive statistics and reporting modules
- Card scheme risk reporting
- Integration with third party monitoring and reporting services

Risk scoring

- Turnkey solutions are integrated with Asseco's Risk scoring module (the InACT Euler® fraud management solution)
- Integration with external risk scoring solutions

End user add-on services

- Enable the user to change risk assessment settings based on personal experience (merchant whitelist, display language, change of available authentication methods, view authentication history list)
- Available as part of Issuer's mobile banking application or as a standalone application

Supported Platforms

(Additional platforms can be supported upon request)

Server Operating Systems
- Red Hat Linux (ver. 6.x, 7.x)
- CentOS (6.x, 7.x)

Application Servers
- WildFly 11+
- WebSphere Liberty 17+

Database Servers
- Oracle (12c, 18c)
- PostgreSQL (9.6+)

Web Server
- Apache HTTPD (2.2.x, 2.4.x)

HSM Devices
- Thales nShield Connect
- Gemalto (SafeNet ProtectServer, SafeNet Network HSM)
- Other HSM types approved by PCI 3DS

Verified by VISA · mastercard ID Check · AMERICAN EXPRESS SafeKey® · Diners Club INTERNATIONAL ProtectBuy · JCB J/Secure · UnionPay 银联

asseco · Payten MEMBER OF asseco