



# Todos eCode

Todos' eCode system is the world's most segmentable, scalable and secure back-end authentication solution for eBanking, eCommerce and mBanking.

Todos VAS - eCode's server and true core - supports a variety of different Two-Factor Authentication solutions based on One-Time Passwords (OTP), Challenge/Response and Electronic Signatures. The system is completely configurable and allows you to combine different authentication schemes with different devices for authentication. This means that by using a Todos eCode setup you can simultaneously use different types of end-user devices and OTP standards.

By deploying Todos VAS with the right eCode add-on modules you may differentiate customers and/or customer needs. Furthermore you can allow one customer to use several devices, i.e. multiple credit/debit cards and let the customer access his services depending on what card is used or even have the same access via different cards. Another eCode add-on enables the system to be configured to service several issuers with separate configurations a.k.a Multi-issuer service.

Advantages	Functionality	Configuration	Standards
<ul style="list-style-type: none"> <li>Solves authentication and secure transactions</li> <li>Handles several millions of user transactions</li> <li>Easy to use, easy to administrate</li> <li>Easy to integrate with existing systems</li> <li>Client API for Call Centre/Web Server/Voice Response</li> <li>Stable, battle proven solution</li> <li>Safe, uses the SSL protocol to protect transaction data</li> <li>Redundant, highly scalable, easy to expand when needed. Just add a server</li> <li>High performance</li> <li>One Central System supports multiple OTP devices of different types</li> <li>The end user may run several tokens, smart card and/or mobile phones in parallel</li> </ul>	<ul style="list-style-type: none"> <li>Verify One-Time Passwords (OTP)</li> <li>Verify Electronic Signatures</li> <li>Dynamic signatures</li> <li>Secure domain separation</li> <li>Multi issuer service</li> <li>Verify Passwords</li> <li>Double Authentication</li> <li>Printed One-Time Passwords</li> <li>SMS sent One-Time Passwords</li> <li>Time limited OTP and challenge/response</li> <li>Personalisation data generation for smart cards and token devices</li> <li>Customer and device database</li> <li>Customer Support Application</li> <li>Key management</li> <li>Audit logs</li> <li>Statistics</li> <li>Supports Radius for VPN/LAN</li> </ul>	<ul style="list-style-type: none"> <li>Windows, Linux or AIX server, IBM main frame</li> <li>Oracle, DB2, MSSQL</li> <li>SafeNet HSM (Hardware Secure Module)</li> </ul> <p><b>Authentication methods</b></p> <ul style="list-style-type: none"> <li>Todos eCode, Todos eCode EMV, Todos eCode Mobile</li> <li>MasterCard SecureCode CAP</li> <li>PLA</li> <li>VISA 3-D Secure</li> <li>German Sm@rt TAN</li> <li>Taiwanese FISC II OTP</li> <li>One-Time Passwords and Electronic Signatures</li> </ul>	<ul style="list-style-type: none"> <li>EMV '96, EMV 2000, EMV 2004</li> <li>MasterCard SecureCode, 3-D Secure CAP, CAP 2007</li> <li>Taiwanese FISC II OTP</li> <li>ISO 13491 (Secure Cryptographic devices)</li> <li>FIPS 140-1 level3 (Security requirements of cryptographic modules)</li> <li>ISO 8732 (Key generation)</li> <li>ANSI X9.32 (Data Encryption Standard)</li> <li>ISO 11568 (Key management)</li> <li>ISO 9797 (Message Authentication Codes)</li> </ul> <p><b>Certifications</b></p> <ul style="list-style-type: none"> <li>MasterCard CAP 2007</li> <li>High-level risk assessment by TNO</li> </ul>