

Solution brief: Connected 3-D Secure resilience

Keep more successfully authenticated transactions moving with Entersekt's ACS and 3DS Server

Digital payments can still fail after a cardholder has successfully authenticated. A disrupted mobile journey, unreliable network or failed browser return can prevent the result from reaching the merchant—leaving an approved customer unable to continue the purchase.

Entersekt strengthens both sides of the 3-D Secure (3DS) journey. Our modernized Access Control Server (ACS) improves authentication completion at the issuer, while our 3-D Secure Server (3DSS) helps ensure that completed authentication results remain available to the merchant when the cardholder's browser does not return them as expected.

Two layers of resilience across the 3DS journey



Issuer resilience

Entersekt's ACS helps more cardholders complete authentication without restarting after interrupted or repeated browser interactions.



Merchant delivery

Entersekt's 3DSS keeps the completed result available when the cardholder's browser does not return to the merchant.

One partner



Entersekt

Two complementary resilience controls across the issuer and merchant sides, supported through one Entersekt relationship.



Production evidence from two leading issuers

Following the introduction of ACS resilience improvements, observed authentication success rates increased across two anonymized issuer deployments.

Issuer deployment	Before	After	Observed improvement
Issuer deployment A	81.7%	88.5%	+6.8 percentage points
Issuer deployment B	77.0%	86.0%	+9.0 percentage points

Production impact: Improving transaction success after authentication

In a separate anonymized weekly production sample, Entersekt's 3DSS resilience improvements increased the proportion of successfully authenticated transactions that could continue processing when cardholder redirection failed.

~41K

authenticated transactions

\$18.4M

authenticated value

1,176

transactions kept actionable

\$423K

authenticated value kept actionable

Entersekt's 3DSS resilience improvements increased the effective transaction continuation rate by approximately 2.9%, keeping 1,176 successfully authenticated transactions actionable when cardholder redirection failed.



A higher success ratio without dependence on browser return

Browser return performance varies with the cardholder's device, network quality, geographic location and the connections between merchant and issuer environments. Entersekt's 3DSS provides an alternative server-side result-delivery path when the primary cardholder-redirect flow does not complete.

The production evidence demonstrates a measurable improvement in transaction continuation: more successfully authenticated transactions remained actionable when browser redirection failed.

What customers gain



More completed authentications:

Greater resilience helps more cardholders complete the authentication journey.



Fewer authenticated transactions lost after challenge:

The result remains available when the cardholder's browser cannot complete the return journey.



A better customer experience:

Customers are less likely to encounter blank screens, interrupted journeys or unnecessary restarts.



Greater operational resilience:

Merchants and processors are less dependent on cardholder devices, browser behavior and network conditions.



One partner across the 3DS journey: Entersekt brings together issuer-side authentication and merchant-side result delivery through complementary ACS and 3DSS capabilities.

Turn authentication success into transaction momentum

Entersekt helps organizations strengthen the complete 3DS journey—from authentication at the issuer to reliable delivery of the result to the merchant.

Strengthen your 3DS journey with
Entersekt's ACS and 3DS Server.

Let's talk

