

RSA Secure.

Providing RSA customers and partners with real-time information on our system performance, security advisories, and other information.

[View ID Plus Status](#)

[View Governance & Lifecycle Status](#)



Detailed Security Information



Security Notices

Detailed security notices for each RSA ID Plus region and service

[Read Notices](#)



Standard Agreements

SLAs detailing system availability and other information





RSA Security Policy

Learn about the security practices, operations, controls, and best practices that secure RSA customers

[Read Notices >](#)

Certification & Compliance.

RSA is certified to comply with industry standards and regulations governing product security, reliability, and availability. We share these certifications as part of our commitment to earning customer trust and delivering proven performance.



FIDO2 Certification

RSA ID Plus is a FIDO2-certified server. The DS100 and RSA Authenticator App 4.4 for iOS and Android are FIDO2-certified authenticators.

[See FIDO certification](#) 



SOC2 Type 2

RSA meets AICPA SOC guidelines requiring CPA issuance of a SOC 2 Type 2 report on controls relevant to security, availability and confidentiality.

Status not applicable to FedRAMP environments.



RSA cloud services have been listed in the Cloud Security Alliance STAR registry since 2017.

[See current status](#) 



FIPS140-2 / FIPS 140-3 compliance

RSA uses FIPS 140-2/FIPS 140-3 validated cryptographic modules for managing data at rest and in motion across mobile apps, cloud, and on-premises.

[Link to certificates](#) 



FedRAMP

FedRAMP

FedRAMP Moderate Authorization for RSA® ID Plus for Government through JAB P-ATO process, making the solution available for US government agencies and Federal System Integrators.

[FedRAMP marketplace](#) 



ISO9001:2015

The quality management system is certified to the ISO 9001:2015 standard in the fulfillment of SecurID Authentication tokens.

[View certificate](#) 



FCC Rules & Regulations for Title 47

RSA hardware authenticators meet FCC guidelines for radiated and conducted emissions in Title 47, part 15 of the CFR.

[See test description](#) 





CE Marking

RSA hardware authenticators meet EU guidelines conforming to directives 93/68/EC: 2004/108/EC: 2006/95/EC: on specifications EN550022 Class A, EN61000-4-2:2008, EN61000-4-3:2006 Class A and RoHS2: EN 50581:2012.

[See EU declaration](#)

[See EC declaration](#)



Cybersecurity & Infrastructure Security Agency (CISA) Secure by Design Pledge

RSA has committed to CISA's pledge and commits to continue creating products that are secure by design.

[View pledge](#)



CISA Secure Software Development Attestation Form

RSA has committed to CISA's Secure Software Development Attestation Form and will continue to leverage secure development techniques and toolsets.

[View form](#)

[View RSAA user guide](#)

Specifications and Standards.



GDPR, CCPA

RSA provides information about some of the applicable aspects described in GDPR and CCPA related to the processing of personal data.

[See privacy considerations](#) 

ACR

Product accessibility information is provided in the Access Conformance Report (ACR), which is a filled Voluntary Product Accessibility Template (VPAT) for given products. This is intended to help clients assess the availability of features that support accessibility.

[Access ACR information](#) 

MIL-STD 810F

Ruggedized testing of RSA hardware authenticators for structural integrity has been conducted in accordance with MIL-STD 810F guidelines.

[See test description](#) 

ISO 13491-1, ISO DIS 13491-2

RSA hardware authenticators comply with ISO 13491-1 and ISO DIS 13491-2 (A2.1.2; A1, A2, A4) standards for being tamper-evident.

[See test description](#) 

Method RS101, MIL-STD-461E

RSA hardware authenticators tested for radiated susceptibility comply with test method RS101, MIL-STD-461E.

[See test description](#) 

UL 913-6th edition (US)

RSA hardware authenticators are designed and tested to the UL 913 standard for safety for use in hazardous locations.

[See test description](#) 

CSA-C22.2 No. 157-92



hazardous locations.

[See test description](#) 

RSA Subprocessors

Information about the Subprocessors that RSA has engaged in accordance with the Data Processing Addendum (DPA).

[See the list](#) 



OpenID® Connect (OIDC)

The RSA OpenID Connect deployment meets OpenID Foundation certifications for interoperability with other implementations. The OpenID Foundation's certification process utilizes self-certification and conformance test suites developed by the Foundation.

[See Certification](#) 

[Basic OP Conformance Details](#) 

[Implicit OP Conformance Details](#) 

[Hybrid OP Conformance Details](#) 

Request a Demo

[Get a Demo](#) 

RSA®

Products

ID Plus

SecurID

Governance & Lifecycle



Partners

Partner Finder

Become a Partner

Partner Portal 

Technical Support
Education Services
Customer Success
Customer Support
RSA Community
Contact Sales

About RSA
Leadership
Webinars & Events
News & Press
Resources
RSA Secure
Careers

Stay Connected with RSA



[Subscribe to RSA >](#)

© 2025 RSA Security LLC or its affiliates. All rights reserved.

[Terms of Use](#)

[Privacy Policy](#)

[Standard Agreements](#)

[Supplier Principles](#)

[Ethical Supply Chain](#)

[ESG](#)

