RSA

WHITE PAPER

Understanding RSA Security

An overview of RSA security practices, operations, and controls

This white paper provides an in-depth security policy review with information about RSA security measures including our practices, operations, and controls centering around our ID Plus offering.

Security and trust are at the heart of everything we do.

The RSA commitment to security

RSA® is trusted by thousands of security-sensitive organizations around the globe to protect hybrid workforces and to accelerate business by delivering secure and convenient access for any user, from anywhere, to anything. Security and trust are at the heart of everything we do. It's core to our products, processes, and people, and it's ingrained into our DNA.

RSA is committed to providing organizations with best-in-class secure, innovative identity solutions that are backed by reliable, unwavering security measures. As a global leader focused on identity and access management, RSA secures sensitive data and enhances the cybersecurity posture of our valued customers.

General security principles

The general security best practices at RSA include:

- A dedicated security risk officer and team leads the overall security posture for all internal resources, products, and commercial services. This team is responsible for establishing, maintaining, and continuously improving the processes, tools, training, and controls used throughout the company. The team performs regular risk assessments on all RSA functions, guides threat modeling, performs periodic scanning and penetration testing of the RSA perimeter, web presence, and software, and leads the investigation into potential vulnerabilities and threats.
- RSA follows best practices for securing our development environment, source code, and build systems including the use of defense in depth, multi-factor authentication, and zero-trust principles for access to all environments. All software is regularly tested with leading third-party analysis tools that are integrated into our development processes and automation.
- RSA products are designed around a fail secure principle that ensures our security controls cannot be bypassed by disrupting communication to security services. For example, if primary authentication services are unreachable, RSA can redirect to redundant software as a service (SaaS) node, to a dedicated on-premises replica (hybrid model), or to local offline authentication. In the unlikely event that none of these options are available, RSA products will fail secure and restrict access.

RSA invests in independent third-party audits and industry certifications to ensure that our products and processes meet or exceed the highest standards. Certification and audit examples include SOC2 Type 2, FedRAMP, CSA STAR, DoD STIG, and FIPS 140-2. For more information, refer to the RSA Certifications and Compliance.[1]

Product and service infrastructure

RSA supports several deployment models, including cloud, hybrid, and on-premises. This range of deployment offers maximum flexibility and ensures secure and reliable operation under any conditions, so organizations can embrace as much, or as little, of the cloud as they choose.

SaaS infrastructure provider

The Cloud Authentication Service from RSA is a multi-tenant SaaS platform hosted on Microsoft® Azure in multiple independent geographic regions including US, Europe, and Australia. RSA uses multi-tenant databases in an environment that shares infrastructure while segregating customer data to ensure privacy. Service levels and operational procedures are standardized for all customers due to the shared nature of the platform. Additional information can be found in the Microsoft Azure Trust Center.

SaaS services infrastructure

The RSA cloud infrastructure consists of a set of services layered on top of each other. Services in the upper layer are more widely accessible but hold the least amount of sensitive information. Services in the lower layers have the most privileges; access to these layers is therefore more strictly controlled. The RSA SaaS operations services are at the heart of this infrastructure and are responsible for monitoring the health of the overall system and performing maintenance procedures, such as product upgrades. SaaS operations require privileged access to the entire service environment and services are performed from an audited, locked down, and tightly controlled system. Remote access to environments is achieved through a secure virtual desktop infrastructure (VDI) system that requires multi-factor authentication

Customer (on-premises) infrastructure

RSA enables customers to protect critical SaaS-based and on-premises web applications, third-party single sign-on (SSO) solutions, and traditional on-premises resources. Communication from the Cloud Authentication Service to on-premises resources (including user stores like Active Directory) is brokered through a secure proxy called the Identity Router (IDR). In high security or air-gapped environments, the RSA® Authentication Manager (AM) can provide authentication, credential and user management services for some or all users entirely on-premises. Both the IDR and AM components are delivered as a hardened security appliance that can be deployed on-premises or in the customer's preferred cloud provider. RSA hardware and virtual appliances include operating system and database components that are specially configured based on US Department of Defense (DOD) Security Technical Implementation Guides (STIG) hardening guidelines. Operating system and database patches are handled automatically and are included in RSA application software updates.

Security controls

Physical access controls

RSA has physical access control systems in place to restrict access to and within RSA facilities.

- Badge access control systems are in place at the perimeter and within the facilities.
- Visitor logs record visitor access to corporate facilities and secure areas.
- Visitors must wear visitor badges while on site and the badges are distinguishable from employee badges.

Data security and encryption

The Cloud Authentication Service uses cryptographically strong encryption and key management to secure sensitive data in transit and at rest. Encryption is secured with FIPS 140-2 approved modules and algorithms, using an AES 256-bit key for data in transit and an AES 256-bit key for data at rest. All connections to and from the Cloud Authentication Service, regardless of data sensitivity, are secured using TLS 1.2 or greater, with ECDHE key agreement, 2048-bit RSA signatures, and AES 256-bit keys. Messages exchanged between the Cloud Authentication Service and the IDR use certificate-based digital signatures and encryption. In addition to the multi-layered encryption, the hybrid deployment model enables RSA customers to keep their most sensitive data on premises and minimize the amount of sensitive data that is sent to the cloud.

Cloud Authentication Service

The RSA Cloud Authentication Service provides the administrative front end to manage the Identity Router, authentication policies, identity sources, and application configuration. The Cloud Authentication Service provides the infrastructure to process authentication protocol requests and interact securely with integrated mobile applications.

The Cloud Authentication Service has several native security features, including network security controls, network segregation, load balancing and high availability, distributed denial of service (DDoS) attack mitigation, host-based intrusion detection system (IDS) and service monitoring.

All communication between service components is encrypted, as is all sensitive data at rest. Security-critical fields in the database are encrypted with tenant-specific keys that cannot themselves be accessed within the database. This approach ensures that security-critical data is not compromised even if an intruder obtains a copy of the database information.

The Cloud Authentication Service is split into multiple tiers across different network segments. Communication between the tiers is restricted to ensure that an attacker that compromises the first tier is not allowed access to subsequent tiers.

Identity Router

The Identity Router (IDR) is a hardened virtual appliance hosted and managed by the customer. The IDR acts as a secure proxy between the customer's on-premises infrastructure (such as Microsoft Active Directory, LDAP v3 directories, and RSA Authentication Manager) and the Cloud Authentication Service. It can also act as web reverse proxy (such as HTTP header integration and password vaulting) or RADIUS server for securing traditional on-premises applications. The IDR ensures that all communication in the hybrid deployment model is managed without directly exposing critical on-premises resources directly to the Internet.

The Identity Router has several security features which include:

- Delivery as a hardened and locked-down virtual appliance. IDR images are downloaded directly from the Cloud Authentication Service, ensuring that latest authorized version is always used.
- All sensitive data is encrypted at rest on the virtual appliance using FIPS 140-2 compliant cryptography. All communication between the IDR and the Cloud Authentication Service is encrypted using TLS v1.2 or better
- Trust between the IDR and the Cloud Authentication Service can be established using a limited-life, one-time passcode generated in the Cloud Authentication Service administration console
- The Identity Router enables a hybrid deployment model where most sensitive data remain on premises and under your control. For example, HTTP Federation (HFED) requires the storage and replay of users' sign-in credentials. Credentials are stored in an encrypted keychain on the IDR, not in the Cloud Authentication Service. Keychains are unique to each user and doubly encrypted with both user-specific keys and a unique tenant key.

RSA Authentication Manager

Deployed on its own, RSA Authentication Manager (AM) is a dedicated on-premises authentication server. In a standalone configuration, AM is a complete authentication solution for traditional hardware and software authenticators based on the RSA One Time Passcode (OTP) algorithm. The AM server is a hardened security appliance available in a range of appliance formats including hardware appliance, VMware, Hyper-V, Amazon EC2, and Azure. It can support deployment in any data center, private cloud, or public cloud environment. Like the Identity Router, AM uses FIPS 140-2 compliant cryptography and TLS v1.2 to secure data in transit and at rest. For organizations that require complete on-premises control and/or operation within secure, air-gapped networks, the RSA Authentication Manager is the de facto solution.

Together with the Cloud Authentication Service and the Identity Router, RSA Authentication Manager can also be used in a hybrid deployment mode bringing together the best of cloud-based agility with on-premises security. RSA Authentication Manager then provides the following additional security benefits:

- Segmented administration – privileged users (and their authenticators) can be segmented from the general user population and managed entirely on-premises
- MFA for legacy applications – AM can act as a secure proxy for RSA Cloud, making modern cloud-based MFA immediately available for hundreds of legacy on-premises applications that already support RSA
- High availability – for on-premises applications connected through AM as a proxy, secure access is maintained even when cloud services are unreachable. These mission-critical applications are always available and always protected

RSA authenticators

RSA supports a broad range of hardware and software authenticators including one-time passcode (OTP) credentials, FIDO, mobile push, and embedded biometrics like Apple Face ID and Microsoft Windows Hello.

The SecurID® 700 Hardware Authenticator is a dedicated OTP hardware credential that meets or exceeds the strictest industry standards for tamper evidence, EMI, ruggedization, and hazardous use. (Additional information can be found at RSA Certifications and Compliance.[2])

RSA also provides an application available on iOS, Android, Windows, and macOS. The application functions as an authenticator for the Cloud Authentication Service or for RSA Authentication Manager. RSA end users can use their devices as a "something you have" authentication factor proven by a push notification or OTP. For multi-factor authentication, "something you know" such as a PIN or "something you are" such as a biometric identifier can be added as well. This application has several native security features that include:

- App package signature verification on installation
- Encryption of locally stored sensitive data
- Encryption of all traffic to and from the Cloud Authentication Service
- Secure enrollment of the device using certificate pinning
- Code obfuscation and anti-tampering defenses
- Detection of jailbroken devices
- Disabling screen sharing
- Credential secrets are stored in the device secure element and cannot be extracted or copied

User data

By design, RSA intentionally limits use of personally identifiable information (PII) and other user data in the Cloud Authentication Service, synchronizing or storing only the minimum attributes required to identify users and to deliver service. Mandatory fields are limited to:

- First Name / Last Name
- Primary username
- Email address
- Primary / secondary unique identifiers (e.g., objectGUID, distinguishedName)
- User Account Status (e.g., active / disabled)
- User Account Expiration

Depending on the ID Plus services enabled, the following fields also may be used:

- Phone number (e.g., for Identity Verification, SMS-based authentication, etc.)
- Manager (e.g., for approver workflows)
- Alternate username (optional)
- Password (cloud users only. Passwords are never synchronized from an external user store)

Customers may also opt to leverage other user attributes in defining role & attribute-based access control policies. In such cases, attributes are queried from the customer's local identity store (e.g. Active Directory), and processed in real-time, but are never stored.

Risk AI is an optional feature that uses machine learning and behavioral analytics to further secure access and reduce the effectiveness of common identity threats by calculating a real-time 'Identity Confidence' score for each authentication attempt. If Identity Confidence is low, for example, RSA may require stronger forms (or multiple forms) of user authentication.

When subscribed for the Risk AI feature, RSA may collect and store the following browser-based data:

- Browser device fingerprint
- ID Address
- Geo-location (collected only with user consent)
- Time of day
- Historical access patterns

To ensure user privacy, all Identity Confidence data is separately stored, encrypted and tokenized to restrict traceability back to individual users

RSA SaaS operations

Personnel access control

RSA has a dedicated SaaS operations team to handle day-to-day maintenance and operation of the product service and infrastructure. RSA maintains geographically distributed operations centers. The service environment is managed through the RSA operations console.

- Access to the operations console is granted only to members of the operations team who are responsible for maintaining the service. Strict separation is maintained between SaaS operations and development environments.
- Employees must complete the operations, security awareness and secure development training before being granted access to the operations console.
- The operation console utilizes a role-based access control system to restrict operator access to functionality that is required to perform that operator's responsibilities.
- All actions performed in the operations console are logged for audit purposes.

Monitoring

Information resources are continuously monitored by SaaS operations personnel to help ensure the secure operation and availability of the system. An internal monitoring system operates 24 hours per day to assess system availability and performance. The system is configured to send real-time notifications to SaaS operations personnel that detail potential issues with the production systems. Network and system activities that are monitored include, but are not limited to, the following:

- Capacity
- Inbound / outbound communications for unusual or unauthorized activities, including the presence of malware such as malicious code, spyware, and adware
- Overloads
- Periods of system unavailability
- Remote access
- Security events and unauthorized activities

Operational and security incidents are recorded and communicated to SaaS operations personnel using the incident response process. As necessary, incidents are escalated for resolution. Continuous monitoring of incidents is performed to help ensure appropriate measures are taken for timely resolution.

Incident response

Documented incident handling policies and procedures are in place to guide personnel in the classification and handling of security events, security incidents, system failures, and breach management. The policies and procedures include the following to guide personnel throughout the incident response process:

- Assignment of roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program
- Containment of the incident and threat
- Mitigating the effects of ongoing security incidents
- Remediation of the incident
- Restoration of operations
- Communication protocols and timing to affected parties
- Lessons learned

SaaS operations personnel are in place to respond to reported incidents. Events identified by internal and third-party providers are required to be reported to SaaS operations personnel. SaaS operations personnel utilize a ticket tracking system to record and monitor security incidents. Incidents that require changes to systems are required to follow change management procedures. Upon resolution of an incident, an after-action report is prepared and provided to management and the affected internal staff. Customer-facing internal staff will notify all affected customers of incidents pertaining to data loss, data corruption, data breach, and/or system unavailability.

Incident response procedures are in place that outline the response procedures to security events and include lessons learned to evaluate the effectiveness of the procedures. The procedures are reviewed annually to help ensure they are effectively meeting the business objectives. Security personnel complete incident postmortem reports for incidents that include incident details and impact analysis, resolutions, lessons learned, and action items.

Business continuity and disaster recovery

RSA has put in place business continuity and disaster recovery plans to guide personnel in procedures to protect against disruptions caused by unexpected events. SaaS operations personnel perform testing of the business continuity and disaster recovery plans annually.

Update and patching

All service infrastructure components are hosted on Microsoft Azure with the most recent security and OS patches. All software updates are tested and approved in the RSA development environment before being applied. After a software update is released, systems are carefully monitored to ensure continued and smooth operation of affected services. RSA also updates the on-premises Identity Router on a regular basis. These updates can be scheduled by the administrator or are deployed on a default date set by RSA.

Configuration and best practices

RSA components and services are pre-configured by default to ensure secure operation in most environments. Depending on your specific use case and need, the flexibility of the products means you can customize deployment, configuration, and security policies. Before changing defaults, RSA recommends that you first read all supporting documentation, consult with your internal cybersecurity team, and ensure that mitigating controls are in place where appropriate. RSA professional services are also available to help in the design and implementation of a new solution or to provide a consultative health check, risk scorecard, and recommendations for any existing deployment.

The Cloud Authentication Service Security Configuration Guide, available from the RSA community website is a good example of supporting documentation.[3]

About RSA

RSA provides trusted identity and access management for 12,000 organizations around the world, managing 25 million enterprise identities and providing secure, convenient access to millions of users. RSA empowers organizations to thrive in a digital world, with complete capabilities for modern authentication, lifecycle management and identity governance. Whether in the cloud or on-premises, RSA connects people with the digital resources they depend on everywhere they live, work and play. For more information, go to RSA.com.

1. RSA Certifications and Compliance https://rsa.com/secure/#certifications
2. RSA Certifications and Compliance https://rsa.com/secure/#certifications
3. RSA SecurID Cloud Authentication Service Documentation https://community.securid.com/s/article/RSA-SecurID-Access-Cloud-Authentication-Service-Security-Configuration-Guide