Ribbon Identity Hub Security and Data Protection

White Paper

Abstract

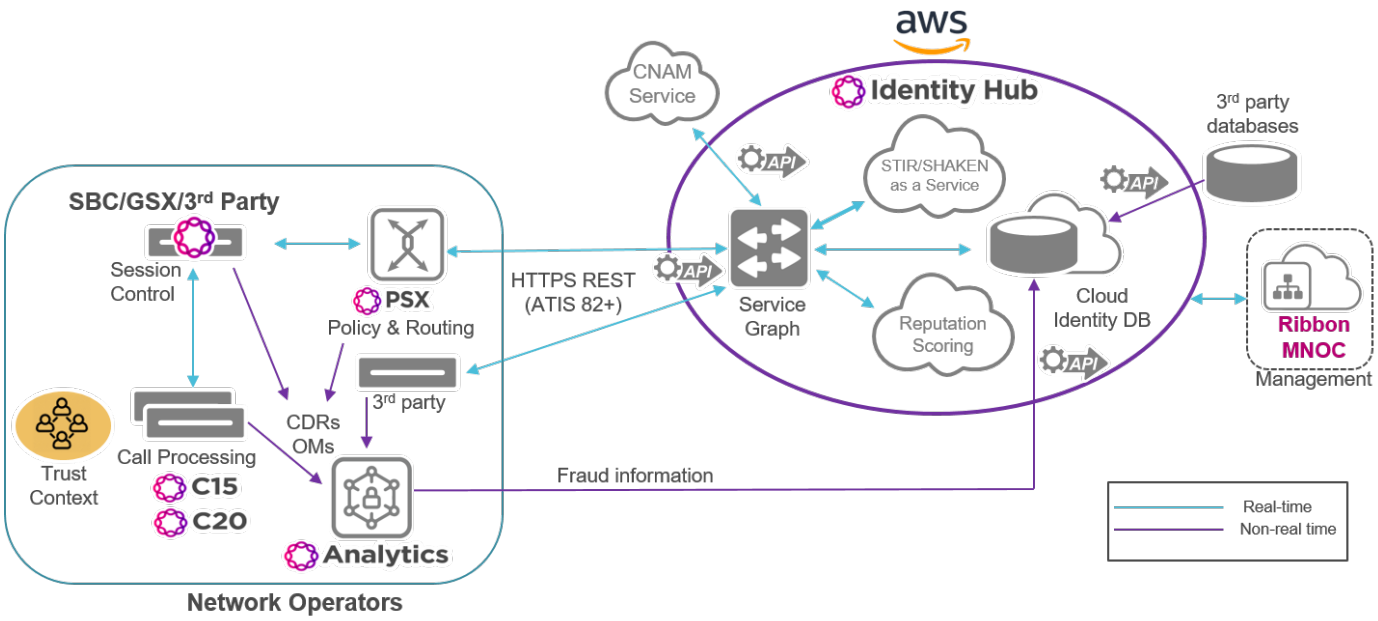
Ribbon Communications has two decades of leadership in real-time communications. Built on world class technology and intellectual property, Ribbon delivers intelligent, secure, embedded real-time communications for today's world. Ribbon's innovative, market-leading portfolio empowers service providers and enterprises with expansive services for their diverse requirements.

Ribbon values the trust that customers place in us to provide their service in a secure and responsible manner. The information in this document provides transparency with regards to security and privacy practices as they pertain to Ribbon's Identity Hub - a fully managed identity assurance services platform hosted in multiple Amazon Web Services (AWS) regions.

While portions of it may apply to other Ribbon service offerings, please consult the respective documents for those services.

Identity Hub Deployment on AWS

The Identity Hub architecture is shown below.



AWS Deployments

Identity Hub is capable of being deployed to any AWS region based on demand; it is currently deployed within the following AWS regions:

Region Code	Name
us-east-1	US East (N. Virginia)
us-west-2	US-West-2 (Oregon)

Network Operator Environment

The portion of the solution within the leftmost bubble labeled Network Operators represent elements of an Identity Assurance solution that are hosted within the operator (customer) environment. This portion is subject to operator's information security practices, policies and controls and is therefore not addressed within this document.

Ribbon-Operated Environment

Identity Hub components below process service data and are subject to Ribbon's security practices including embedded design security, privacy characteristics as well as operational information security frameworks and practices. These security practices function in concert with complementary data center security controls offered by AWS.

Component	Description
Identity Hub	Cloud-hosted components hosted in multiple Amazon Web Services (AWS) regions.
Ribbon MNOC	Ribbon Managed Network Operations Center (MNOC) provides 24x7x365 operational control of Identity Hub including monitoring of ongoing availability, integrity and security of the service. MNOC personnel are also responsible for customer onboarding procedures.

Third Party Data Sources

Identity Hub will ingest certain data from third party data sources including Nomorobo, PRISM (FRS Labs) and LERG6 (Iconectiv).

Security and Privacy by Design

This section summarizes Identity Hub's security and privacy by design attributes.

Service Data - Ribbon Managed

The following table provides a summary of Ribbon-managed service data within Identity Hub.

Data Type	Retention	Description
TDR	Maximum 15 Months	Identity Hub Transaction Data Records (TDRs) will contain caller and called party telephone number and caller ID
Third Party Database Snapshots	Subject to Third Party Database Provider Update Frequency and Retention Controls	Downloaded copies of third-party databases (eg: PRISM, Nomorobo)
Billing Information	Minimum 7 years	Daily aggregated tenant service billing information.

The scope and retention of service data processed within Identity Hub has been minimized to align to the following purposes:

- Reliability and performance of Identity Hub algorithmic outcomes
- Resolving any billing disputes
- Calculating and delivering yearly true-ups
- Historical usage analysis for performance tuning and product improvement using aggregated data
- Compliance with applicable laws and regulations

Service Data - Customer Managed

The following table provides a summary of customer-managed service data within Identity Hub.

Data Type	Retention	Description
Tenant Allow List	Subject to Customer's Update and Retention Controls	Telephone numbers that should be treated as low likelihood for nuisance or fraud.
Tenant Deny List	Subject to Customer's Update and Retention Controls	Telephone numbers that should be treated as high likelihood for nuisance or fraud.
Tenant Does-Not-Originate List	Subject to Customer's Update and Retention Controls	Telephone numbers that do not originate calls; treated as high likelihood for nuisance or fraud.
Tenant Fraud List	Subject to Customer's Update and Retention Controls	Telephone numbers that should be treated as high likelihood for fraud.

Secure Development Process

The Ribbon software development and deployment process follows an Agile development methodology. The process natively incorporates secure-by-design principles during the planning, design, implementation, testing, and operational phases. Ribbon follows industry standard practices with respect to protecting data, authenticating and authorizing use, and providing monitoring and auditing capabilities as intrinsic facilities.

Activities and processes promoting our secure-by-design principles include:

- Design checklists in line with best practices from OWASP and similar software security frameworks
- Peer review of all code that incorporates security guidelines validation
- Mandatory annual security training for all development, testing, and operations personnel
- Internal threat assessment modeling and mitigation reviews prior to product launch
- Security and risk review with cloud service provider (AWS)
- Penetration testing by a recognized third-party security vendor
- Continuous synthetic traffic testing for security (and functional) validation

Defense-in-Depth

Identity Hub is organized into separate management planes and service planes, with each plane in a separate Virtual Private Cloud (VPC). Within each VPC, the connection to the Internet is through an AWS managed service (Application Load Balancer or API GW); additionally, an S3 bucket for tenant list uploads is accessible through pre-signed URLs allocated as part of an authenticated upload request.. All backend services are in separate networks with no direct access to anything but the Identity Hub's service consumer components.

Identify Hub is not reachable by the general public. Customer access is explicitly enabled as part of a secure onboarding process and access is restricted to their provided IP Classless Inter-Domain Routing (CIDRs) for management and service processing clients. Identity Hub also provides VPC-to-VPC access for customers desiring access from their AWS VPC. Such connections are enabled on a per-customer-AWS-account basis, and traffic for such connections is exchanged directly within AWS and does not traverse the Internet.

Tenant Account Security

Identity Hub tenant accounts are protected through separate management plane and service plane API keys. The initial management API key is generated and provided to the customer as part of Identity Hub onboarding procedure. The service API key is then be generated using a management API request using the management API key. All management REST requests require that the management API key be provided in the Authorization header and, similarly, all service REST requests require the service API key.

Best practice requires that the customer immediately rotate the initially provided management API key and subsequently at regular intervals thereafter. Similarly, the service API key should be also rotated regularly by the customer. To facilitate operations related to API key rotation, the service will accept the prior API key for a short grace period after key rotation. Ribbon does not save the customer's API keys in plaintext. Instead, appropriately salted and hashed versions are maintained for future authentication. Consequently, Ribbon is unable to recover a lost API key but can instead assist in resetting the keys via an appropriate out-of-band authentication method.

Data Encryption in Transit

All external interfaces to Identity Hub are TLS encrypted HTTPS only connections. No unencrypted protocols (ex: HTTP) are supported.

All internal data traffic is transported via VPC tunnels within a private VPC. The traffic is secure (cannot leave the VPC except through a service specifically added for cross-VPC access) and private (cannot be viewed by a different AWS tenant).

Data Encryption at Rest

All data at rest is protected using industry standard AES encryption. This includes service data within databases as well as data in object stores. Keys are managed through the AWS KMS service, a FIPS 140-2 compliant service. Keys are never stored in plaintext and never leave the AWS region in which they were created. Certain sensitive data, such as STIR/SHAKEN signing keys, are further "envelope encrypted" with the data keys managed by the AWS KMS service.

Vulnerability Management

Identity Hub software and included open source packages are scanned for vulnerabilities at multiple points in the secure software development and deployment process. Initial scans are performed as part of the build pipeline, and secondary scans are executed at the point of adding Docker container images to the AWS Elastic Container Registry (ECR).

On a periodic basis, all Docker container images in the AWS ECR for Identity Hub are rescanned against the most current vulnerability fingerprints. Any newly discovered vulnerability triggers an operations action to replace all containers running that image with the most current (i.e. without the vulnerability) image.

Logging and Audit Trails

The service incorporates comprehensive centralized logging and audit trails covering the full breadth of Identity Hub. This includes logging and KPIs associated with the application proper as well as information related to the underlying cloud infrastructure. All information is logged centrally and associated with alarms and KPIs monitored by the Ribbon Managed Network Operations Center (MNOC) personnel.

Information logged includes (but is not limited to): access logs for all management plane activities; all application and infrastructure configuration activities; all external activity to data stores; KPIs tracking service usage, data flows, compute utilization; and internal security key usage.

Logs are maintained for at least 90 days, with certain types of logs and audit information maintained at least 6 months.

Access to logs and audit trails are restricted to Ribbon personnel with role-based access that have been combined with granular access limits based on the type of data logged.

Continuous Service Monitoring

Identity Hub incorporates continuous monitoring of availability and security through synthetic designed traffic. This process detects both functional failures and improper or unauthorized accessibility of services. The results of this continuous monitoring are reviewed and evaluated through regular audits of the service by Ribbon personnel.

Service Resiliency

Ribbon's Identity Hub provides complete business continuity across a full range of contingency events including:

- **isolated compute**
- **networking or data resource failure**
- **entire data center failure**
- **catastrophic events affecting very large regions (such as the entire USA eastern coast).**

Uptime and Availability

Identity Hub is implemented in multiple AWS availability zones (AZs) within a deployed-to AWS region. Within an AZ, all resources are auto-scaling and auto-replaceable. Within a region, each AZ comprises one or more data centers, with each AZ residing on independent power grid cells, flood zone, and earthquake fault zone and separated from each other by at least a few miles. Identity Hub is automatically and transparently fault tolerant to individual resource failure or entire data center or AZ failure. Additional information regarding the AWS global infrastructure can be found here.

Identity Hub is also implemented in multiple AWS regions. Customer traffic to Identity Hub is distributed through AWS Route-53 DNS, configured with health-checking. Consequently, failure event impacting an entire region is transparently fault tolerant provided the client equipment follow best practices on DNS resolution.

The reader should note that Identity Hub is designed to be fault-tolerant, not just redundant. In particular, the service provides full service capacity during fault events. Additionally, for events which do not result in regional re-routing, the service latency characteristics will be unaffected. For fault events causing regional re-routing, Identity Hub service latency itself is unchanged - however the customer may experience increased latency due to additional networking delays to the alternative region.

Data Backups

Identity Hub is configured to perform regular backups of all customer account information including service configuration, operational metrics, and metrics associated with billing. These backups are available for at least 30 days. Additionally, service data including transaction records and billing records are stored in versioned object stores.

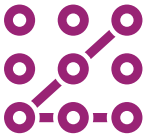
All backup data is encrypted at rest and replicated across multiple AWS availability zones.

Security for Operations

Ribbon maintains the secure operation of Identity Hub within the context of the AWS shared security responsibility model. For more information regarding the AWS shared security model, please refer to AWS' Introduction to AWS Security whitepaper.

Ribbon's Identity Hub is hosted in AWS data centers. Hosting includes both Identity Hub itself as well as customer data associated with the Identity Hub services. AWS-hosted data centers are world-class and are compliant to numerous recognized industry operational security standards (including ISO 27001, ISO 27017, ISO 27018). AWS also maintains SOC-2 and SOC-3 attestations in the regions where Ribbon Identity Hub is deployed. Additional AWS standards compliance information can be found here.

Ribbon maintains “Security in the Cloud” security practices which function in concert with AWS hosting data center controls and which are aligned to industry standard. In practice these apply to the Ribbon-operated environment described above. Ribbon has a dedicated Managed Network Operations Center (MNOC) and Production Engineering team responsible for the ongoing operations and security of Identity Hub. This team includes at least one security principal responsible for the security aspect of operations, and is responsible for auditing, security compliance, and incident response.



Physical Access (MNOC)

Identity Hub is managed from MNOC which is located within Ribbon’s Prague (Czech Republic) facility. The location is subject to corporate security measures including access controls designed to limit facility and MNOC access to authorized individuals. These security measures include requirements for identification and access cards and CCTV. Access to the MNOC itself requires elevated privileges which is strictly controlled by Ribbon management.

Logical Access

Access to Identity Hub AWS infrastructure is subject to Ribbon’s access control policy and is further subject to IP filtering controls. Ribbon maintains a record of security privileges of individuals having access to Identity Hub and has implemented industry standard practices to identify and authenticate Ribbon personnel who attempt to access the Identity Hub systems including a 3-tier role-based access model based on principle of least privilege. Authorized Ribbon personnel who have been granted access to the Identity Hub infrastructure are assigned the appropriate role which is associated with their unique userID which is in turn subject to corporate federated access (SSO) controls. Each user must maintain a complex password which must be renewed regularly and no less frequently than 90 days. Ribbon ensures that user access to the Identity Hub environment is promptly de-activated when it is no longer required. A regular access review is undertaken by Ribbon at a minimum on a quarterly basis.

Access via the root account is lock-boxed and requires additional Multi-Factor-Authentication (MFA). The root account is never used in the normal course of operation.

Access to the Identity Hub service level API is restricted to clients within the MNOC VPC. To reach an existing client, MNOC personnel must first access a jump server in the public portion of the MNOC VPC. Only MNOC personnel have accounts on this jump server, account access is strictly key based, and the server only allows connections from whitelisted IP addresses. Only MNOC admin personnel can create accounts on the jump server after approval by management.

Service Administration

Administration of the Identity Hub service level configuration (in contrast to tenant-level configuration) is restricted to only client software within the MNOC VPC. Access to these clients, or roles allowing instantiation of new clients in the MNOC VPC is limited to Ribbon MNOC personnel with appropriate roles. Consequently, configuration changes to production service is restricted to MNOC personnel with administrative level privileges.

Change Management

Ribbon adheres to a defined change control process for the deployment of new code to Identity Hub. Deployment is controlled through a Continuous Deployment (CD) pipeline. This pipeline first deploys code to a "solution test" environment for end-to-end testing. If successful, deployment is then initiated against a "staging" environment. Finally, if and only if the prior deployments and subsequent testing are successful, code changes are deployed to the production environment, in sequential order.

Deployments of new code to an environment follows a blue-green model with canary or linear testing of traffic. This ensures stability and functionality with a limited set of production traffic before roll-out to the full capacity production systems. Rollback to the prior release is automatic upon detection of traffic error or by manual operation by monitoring personnel.

Configuration changes also follow a defined change process. All service level configuration is captured between configuration in a database or configuration commands securely held in a version control system. Before any configuration changes are made, a point-in-time (PITM) backup of the configuration database is made and/or changes are made to the version-controlled action scripts and the scripts saved. All configuration changes are peer-reviewed and approved before being applied and tested. In the event of unforeseen issues, the PITM backup is restored and/or the prior version of action scripts applied, as appropriate.

Security Monitoring and Incident Handling

Ribbon security personnel review event logs within Identity Hub upon security event triggers and also on a bi-weekly audit basis. In the event of a security incident, Ribbon's security incident response process is invoked. Key incident lifecycle and risk mitigation aspects of this process include:

- the categorization and severity ranking criteria for security events
- the triggers for investigation
- flowcharts of processes to be followed by investigating personnel
- roles and responsibilities of various personnel
- relevant external party engagement
- notification guidelines and requirements to customers and where applicable governmental organizations
- mitigation options

Appropriate Ribbon personnel have been trained to maintain and oversee the security incident response process.

Penetration Testing

Ribbon engages a reputable third-party provider to conduct regular penetration testing of Identity Hub. This activity includes penetration testing of the management and service APIs as well as examination and penetration testing of the infrastructure configuration.

Human Resources Security

Ribbon informs Identity Hub personnel about relevant security obligations, procedures, and their respective roles. Ribbon maintains an Identity Hub personnel security posture characterized by the following human resource security practices.

- Personnel are party to confidentiality terms as part of the onboarding process and must regularly attest to compliance to Ribbon code of conduct
- Mandatory annual secure coding practices training for developers
- Mandatory corporate information security and data protection training

Data Protection and Compliance

Privacy by Design

Ribbon has considered the data protection principles and implemented appropriate technical and organizational measures such as those described in the preceding sections of this document. These measures have taken into account the state of the art, the cost of implementation and the nature, scope, context and purposes of service data processing as well as the risks of varying likelihood and severity of a security incident leading to a personal data breach.

Data Protection Regulatory Compliance

Ribbon is committed to protecting the personal data of its customers, partners and affiliates wherever it does business around the globe. This commitment is underpinned by the implementation of industry best practices for information security and the application of data protection controls supportive of applicable global privacy laws and data protection regulations. Ribbon maintains an active privacy program that is aligned to industry standards and maintains a corporate membership within the International Association of Privacy Professionals (IAPP) - the largest and most comprehensive global information privacy community and resource. Readers are also encouraged to review Ribbon's Privacy Policy for further insight on Ribbon's approach to data protection.

EU GDPR Accountabilities

In anticipation of Identity Hub becoming available in jurisdictions subject to the EU General Data Protection Regulation (EU) 2016/679 ("EU GDPR"), Ribbon has applied a privacy by design (PbD) approach to design of Identity Hub.

In terms of data protection obligations, Ribbon is considered a "data processor" within the context of Identity Hub and is committed to supporting Identity Hub customers and partners with their respective "data controller" compliance obligations under the EU GDPR . Ribbon is able to promptly enter into Data Processing Agreement (DPA) terms with customers supportive of ongoing compliance requirements reflected in the GDPR including Article 28(3).
The following are some sample Identity Hub solution attributes which are supportive on ongoing EU GDPR compliance:

- Hosting of Identity Hub within the EEA prior to service becoming available in GDPR jurisdictions
- A comprehensive suite of corporate data protection policies and controls
- Maintenance and expansion of an ISO27001 program within Ribbon in support of Article 32
- Maintenance of privacy measures aligned to industry frameworks such as ISO27701.
- Adoption of OneTrust™ privacy management software to operationalize the data protection program
- Intra-Ribbon group standard EC data protection clauses (SCCs)
- Article 30 mapping personal data processing activities and underlying assets
- Personal Data Breach response protocol (SIRP-B) in support of Articles 33 and 34
- Vendor risk management program – regular vendor risk reviews and targeted engagements
- Delivery of regular, corporate-wide privacy training based on IAPP eCore content
- Targeted Data Protection Impact Assessments (DPIAs)
- Support of customer DPIA activities and questionnaires
- Support of customer in fulfillment of applicable Data Subject Rights (DSR) under GDPR Chapter III

Contact Ribbon today to learn more about Identity Hub Security and Data Protection

About Ribbon

Ribbon Communications (Nasdaq: RBBN), which recently merged with ECI Telecom Group, delivers global communications software and network solutions to service providers, enterprises and critical infrastructure sectors. We engage deeply with our customers, helping them modernize their networks for improved competitive positioning and business outcomes in today's smart, always-on and data-hungry world. Our innovative, end-to-end solutions portfolio delivers unparalleled scale, performance, and agility, including core to edge IP solutions, UCaaS/CPaaS cloud offers, leading-edge software security and analytics tools, as well as packet and optical networking leveraging ECI's Elastic Network technology.