SOC 3 for Security, Availability, Processing Integrity, and Confidentiality

Independent Practitioner’s Trust Services Report

For the Period May 1, 2013 through October 15, 2014

zixcorp
# Table of Contents

**SECTION ONE:**  
INDEPENDENT PRACTITIONER’S TRUST SERVICES REPORT ................................................................. 1

**SECTION TWO:**  
ZIXCORP’S ASSERTION REGARDING ITS SYSTEM ............................................................................ 3

**SECTION THREE:**  
DESCRIPTION OF ZIXCORP’S SYSTEM .......................................................................................... 4
SECTION ONE: INDEPENDENT PRACTIONER’S TRUST SERVICES REPORT

To the Management of Zix Corporation:

Scope
We have examined management’s assertion that during the period May 1, 2013 through October 15, 2014, ZixCorp (the “Company”) maintained effective controls over its ZixPort, ZixONE, and Hosted Services system, based on the American Institute of Public Accountants (“AICPA”) and Chartered Professional Accountants of Canada (“CPA Canada”) trust services security, availability, processing integrity, and confidentiality criteria to provide reasonable assurance that:

• the system is protected against unauthorized access, use, or modification;
• the system is available for operation and use as committed or agreed;
• the system processing is complete, valid, accurate, timely, and authorized; and
• the system information designated as confidential is protected as committed or agreed.

The Company is responsible for this assertion. Our responsibility is to express an opinion based on our examination. The Company’s management description of the aspects of the ZixPort, ZixONE, and Hosted Services system covered by their respective assertion is outlined within the report.

Our examination was conducted in accordance with attestation standards established by the AICPA and, accordingly, included (1) obtaining an understanding of the Company’s relevant controls over security, availability, processing integrity, and confidentiality of the ZixPort, ZixONE, and Hosted Services system; (2) testing and evaluating the operating effectiveness of the controls; and (3) performing such other procedures as we considered necessary during our examination. We believe that our examination provides a reasonable basis for our opinion.

Because of the nature and inherent limitations of controls, the Company’s ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct errors or fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

In our opinion, the Company’s assertion referred to above are fairly stated, in all material respects, based on the AICPA and CPA Canada trust services security, availability, processing integrity, and confidentiality criteria.
ZixCorp’s use of the SysTrust for Service Organizations Seal constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to update this report or provide any additional assurance.

SSAE 16 Professionals, LLP

November 17, 2014
Orange, California
SECTION TWO: ZIXCORP’S ASSERTION REGARDING ITS ZIXPORT, ZIXONE, AND HOSTED SERVICES SYSTEM

November 17, 2014

During the period May 1, 2013 through October 15, 2014, the Company, in all material respects maintained effective controls over the ZixPort, ZixONE, and Hosted Services system, as defined by the ‘System Description’ attached within the report, to provide reasonable assurance that:

• the system is protected against unauthorized access, use, or modification;
• the system is available for operation and use as committed or agreed;
• the system processing is complete, valid, accurate, timely, and authorized; and
• the system information designated as confidential is protected as committed or agreed.

Further, the Company confirms that to the best of our knowledge and belief, that the controls related to the trust services security, availability, processing integrity, and confidentiality criteria were suitably designed and operating effectively during the period May 1, 2013 through October 15, 2014, to achieve those control objectives. The criteria we used in making this assertion were that:

• The risks that threaten the achievement of the controls related to the trust services criteria have been identified by the Company; and

• The controls related to the trust services criteria would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the trust services criteria from being achieved.

ZixCorp
SECTION THREE: DESCRIPTION OF ZIXCORP’S SYSTEM

1 Overview of the System and Applications

ZixCorp provides email encryption services for privacy and regulatory compliance with over 43 million protected email recipients including encrypted email delivery to healthcare organizations, financial institutions and government agencies. ZixCorp supports five encrypted email delivery mechanisms including S/MIME, TLS, OpenPGP, secure portal and "push" delivery.

Description of ZixData Center℠

_ZixData Center_, located in Dallas, Texas with a backup facility in Austin, Texas, has the capacity, scalability and infrastructure to support encryption keys for every email address in the world. _ZixData Center_ is staffed 24-hours a day with operations personnel monitoring the facilities, networks, systems and applications. The physical security of the _ZixData Center_ employs a five-layer security approach. Access to the _ZixData Center_ is controlled through a series of doors that employ access controls such as 24-hour security guards, electronic badge readers and biometric devices used in combination with a badge reader. Operations staff has been carefully screened, including background checks performed by an external investigation firm.

Uninterrupted electrical power is required for the continuous operation of servers, communication equipment and environmental controls. ZixCorp’s policy of complete redundancy has been designed to ensure there are no potential single points of failure throughout the data center for any given system component. Two independent high-bandwidth fiber trunks move traffic in and out of the data center to three independent internet service providers.
ZixData Center Key Benefits:
- Redundant electrical feeds from independent utility power grids
- Redundantly configured fiber connections and redundant routers
- Dual uninterruptible power supplies
- Sun Microsystems Solaris-based systems and Intel Linux-based systems
- Back-up diesel generator
- Scalably web server architecture
- Redundantly configured power distribution units
- 99.99% reliability
- Multiple ISPs

Description of ZixCorp Services – BYOD

ZixOne\textsuperscript{SM}
ZixOne is the Bring Your Own Device (BYOD) solution that bridges the gap between enterprise security and expense concerns and the growing preference among employees to maintain a single mobile device for office and personal use. For organizations, ZixOne satisfies security requirements by allowing organizations to keep their data stored on their servers and control employee access. ZixOne eliminates the need for organizations to purchase, maintain and issue mobile devices or services to employees. It also significantly reduces legal exposure to privacy issues. For employees, ZixOne offers the ability to manage both personal and enterprise data on a single mobile device without losing convenience, control or privacy with their personal mobile devices. Employees can choose from a variety of iOS® or Android™ mobile devices.

Organization administrators can immediately suspend mobile device access to the ZixOne server using the browser-based Administration Console. Administrators can use the Administration Console to limit ZixOne usage to an exclusive access list. Searchable mobile device activity logs on the console's Reports screen give administrators monitoring and diagnostic capabilities as well.

ZixONE Key Benefits:
- No corporate data on device
- Simple, secure connection to the office
- Seamless user experience
- Employee privacy and control
- Per user pricing

ZixONE Key Features:
- Android and iOS compatible
- High-efficiency protocols deliver data quickly and securely
- Easy administration controls for disabling access
• Reporting capabilities for improved regulatory compliance

Description of ZixCorp Services – Email Data Loss Prevention

ZixDLP
Email is the most used communication tool in business. It enables organizations to conveniently collaborate and share valuable information, from customer data to intellectual property, inside and outside an organization’s network. With ZixDLP, an email data loss prevention tool, your organization can monitor and protect the channel that both assists your company in running efficiently and exposes your organization to the most risk. Leveraging ZixCorp’s leadership and expertise in email encryption, ZixDLP combines our proven policy and content scanning capabilities with an intuitive quarantine interface. ZixDLP provides you with the ability to:

• Use ZixGateway policies to quarantine email that contains sensitive information.
• Scan outbound email messages for violations based on sender, recipient, subject, body and attachments using lexicons, file types and other filters.
• Process quarantined email messages by:
  • Creating authorized users who can process quarantined messages.
  • Reviewing policy and content violations for a quarantined message.
  • Searching and filtering messages, assigning category labels and applying comments.
  • Releasing and deleting multiple quarantined messages concurrently.
• Sending notification messages to employees regarding quarantined emails.
• Review quarantine reports using the ZixReporting Dashboard.
ZixDLP Key Benefits:
• Easy to use and cost-effective
• Enhanced visibility into sensitive information in outbound email
• Strengthened compliance with corporate policies
• Improved employee education regarding the treatment of sensitive information

ZixDLP Key Features:
• Powerful administrative capabilities
• Intuitive administrative dashboard
• Reporting of quarantine activities and trends
• Deployable as a bundled, ad-on or standalone solution

Description of ZixCorp Services – Email Encryption

ZixGateway™
ZixGateway is a policy-based email encryption service that uses an appliance for enterprise-wide regulatory compliance. It provides company-wide security, content filtering, and management of outbound corporate email. ZixGateway provides the benefits of a secure messaging gateway without having to create and manage encryption keys, by leveraging the email encryption directory, ZixDirectory. Plus, it is totally transparent to end users.

ZixGateway enables organizations to comply with industry regulations and corporate security policies with built-in lexicons that automatically encrypt messages to meet specific needs including healthcare, finance, and profanity. ZixGateway provides a secure and private channel for email communications between employees, customers, and business partners — or anyone with an email address. ZixGateway employs efficient and secure ways to deliver messages through ZixCorp’s unique Best Method of Delivery.

Superior support for TLS
The latest version of ZixGateway also offers unique support for TLS in several ways. TLS through ZixGateway provides:
• Secure, bidirectional transparency - ZixCorp Best Method of Delivery chooses the most secure and transparent delivery method available for each message. ZixCorp S/MIME provides high security and bidirectional transparency. If S/MIME is not available, TLS can be configured as an alternative transparent delivery method.
• Simplified set-up of mandatory TLS - By making TLS a part of the email encryption policies, TLS can be added as a delivery method by simply checking a box. By replacing the need for individual TLS configurations, ZixGateway allows your organization to skip the cost and time typically associated with each connection.
• Increased delivery control - No longer is TLS an all-or-nothing method. By making TLS a part of the ZixGateway policies, TLS is used only where appropriate.
• Reporting capabilities - ZixGateway offers superior visibility for compliance officers by providing reports that log how each message was delivered, including TLS encrypted email, and who it was delivered to.
• Branding of recipient messages - Embedded at the bottom of each TLS message is a "Secured by ZixCorp" note, providing confidence to your recipients that the email and its sensitive content were delivered securely.

Secure, bidirectional transparency, increased control, increased visibility and unique branding are features not available in competing TLS solutions.

Flexible Delivery
For recipients who do not have email encryption capabilities, ZixGateway offers two different delivery methods - ZixPort and ZixDirect. All of these options combine to create the ZixCorp Best Method of Delivery, which automatically determines the most secure and transparent method of sending your message.

Best Method of Delivery

ZixGateway Key Benefits:
• Offered an your location as an appliance or as a hosted service
• Quick deployment in less than a day
• Ability to send secure email to anyone
• No training for end users
• Implemented as an appliance or as virtual environment application
• Built-in content scanning
• Seamless integration with existing infrastructure and systems
ZixGateway Key Features:

- Full content scanning of message and attachments
- Centralized policy management
- Automatic retrieval and distribution of public encryption keys through ZixDirectory
- Corporate-defined policy management
- Flexible reporting capabilities
- Custom branding
- Message and attachment compression
- Interoperability with S/MIME and OpenPGP
- Support of TLS and SSL protocols
- Secure receive and reply for all recipients

ZixGateway - Inbound and ZixGateway - Access can be provided as alternative services to provide certain subsets of ZixGateway capabilities based on the client’s needs.

ZixGateway - Inbound
The Health Information Technology for Economic and Clinical Health (HITECH) Act, passed as part of American Recovery and Reinvestment Act of 2009 (ARRA), calls for protected health information (PHI) to be rendered unreadable and unusable. Under the new legislation, healthcare organizations can be fined up to $1.5 million for violating the rules protecting patient privacy. Their business associates are also covered as part of the most recent changes.

For many healthcare organizations, safeguarding email sent by its employees is not enough. They also want to proactively identify any potential vulnerability. ZixCorp Email Encryption Services are an important solution in the protection of sensitive data, and now ZixGateway Inbound provides a way for healthcare organizations to better manage their compliance with HITECH and the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

With ZixGateway Inbound, inbound email is content-scanned for unsecure PHI. When vulnerabilities are identified, both the business associate and the appropriate internal compliance manager can be automatically notified. In addition, ZixGateway Inbound provides reports that log the details of inbound vulnerabilities. The reports can be sent to the compliance or security staff on a daily basis for additional review and action. This enables healthcare organizations to proactively identify vulnerabilities, as well as protect their patients and their brand.

ZixGateway – Inbound Key Benefits:

- Proactively identifies inbound email PHI breaches
- Inbound HIPAA content scanning

ZixGateway – Inbound Key Features:

- Policy management for HIPAA compliance
- Full content scanning of message and
ZixGateway - Access

ZixCorp has become a leader in email encryption services by offering superior technology to some of the nation’s most influential institutions. ZixAccess provides secure, transparent communication to those institutions and your most valuable customers and partners. Enabled through ZixDirectory® – the email encryption network – ZixAccess automatically decrypts inbound email from ZixCorp users and provides transparent communication with no password required. Transparent Email Encryption ServicesSM removes the extra steps of push and pull messaging to improve productivity for all your email users.

The Value of the ZixDirectory

ZixDirectory includes tens of millions of members, increases at approximately 100,000 members per week and has the power to manage the encryption keys for every email address in the world. ZixDirectory is housed in the ZixData Center™ with 99.99% availability guaranteed in ZixCorp service level agreements. By leveraging ZixAccess, you are automatically enrolled in the ZixDirectory and instantly benefit from transparent email encryption with other ZixCorp users.

Lexicon Scanning

In addition to the advantages of transparent inbound communication, ZixAccess provides improved visibility for sensitive outbound email. ZixAccess features the capability to automatically scan all outbound email with ZixCorp’s proven lexicons. As a second line of defense against unsecure sensitive information in transit, ZixAccess will report all outbound risks to your security or compliance officer.

Enhanced User Productivity

ZixAccess eliminates the need for internal employees to click on a link or attachment and enter a password to access messages encrypted by other ZixCorp customers. ZixAccess automatically decrypts the messages after they enter your secure network, making it possible for employees to read the message directly in their inbox without a password. If your employee replies to a message from a ZixCorp customer, ZixAccess can ensure the message is encrypted before it leaves your network, maintaining the confidentiality of the contents.

- Quick deployment in less than a day
- Implemented as an appliance or as virtual environment application
- Seamless integration with existing infrastructure and systems
- User accounts automatically enrolled
- Automated breach notifications
- Daily policy breach reports
- Attachments
ZixGateway – Access Key Benefits:

- Access to tens of millions of ZixDirectory members
- Transparent decryption with no password required to view secure email
- Increased visibility into outbound email
- Easy upgrade to ZixGateway outbound email encryption

ZixGateway – Access Key Features:

- Available as a virtual or physical appliance
- Installation, configuration and maintenance included as service
- Hosting of public key in shared ZixDirectory
- Automatic decryption from ZixGateway and ZixMail customers
- ZixCorp lexicon scanning and compliance alerts of unsecure outbound email with sensitive information

ZixMail®

ZixMail is a desktop email encryption solution that provides individuals with a high level of security. It is an easy-to-use service that enables users to encrypt and decrypt emails and their attachments to anyone, with a single click. ZixMail can be downloaded and installed in minutes and integrates with all corporate email systems. The service provides automatic retrieval and distribution of public encryption keys through ZixDirectory. For extra convenience, certified receipts help senders know exactly when messages were sent and opened. ZixMail utilizes ZixCorp’s Best Method of Delivery, if the recipient is not an existing ZixCorp customer, ZixMail will automatically send the message to a ZixPort® secure portal, ensuring emails can be securely sent to any user, anywhere.

ZixMail Key Benefits:

- Easy to use
- Fast and easy to deploy
- Ability to send to anyone
- End-to-end delivery assurance
- No hardware to install
- Automatic public key exchange through ZixDirectory
- Compliant with existing systems

ZixMail Key Features:

- User-controlled operation
- Date- and time-stamped certified receipts
- Secure message storage
- Message and attachment compression
- Fully integrated version for Microsoft® Outlook®
- Requires minimal IT support
- Creation of certified receipts and non-refutable time stamps

ZixPort®

ZixPort is a secure messaging service that provides companies with a way to encrypt email communications with their customers and business partners. As a hosted service, branded for each customer, ZixPort does not require additional information technology (IT), web or security infrastructure. ZixPort is based on standard internet technology ensuring users can
access their secure messages through a variety of browsers including browsers on mobile devices. With ZixPort, customers can customize the look and feel to match their web site and select from a variety of features to meet their needs. As a hosted solution, ZixPort requires little internal resource support, development time or hardware and it is easy for employees, customers and business partners to use. ZixPort is hosted in the ZixData CenterSM for optimal security and availability. It also takes advantage of ZixCorp’s unique Best Method of Delivery and provides send-to-anyone capabilities for both ZixGateway and ZixMail.

**ZixPort Key Benefits:**

- Branding customization based on your organization’s needs
- No software or user training needed
- Secure message send capability to anyone, anywhere
- No impact on internal IT resources or infrastructure
- Feature customization for optimum flexibility

**ZixPort Key Features:**

- User-controlled operation
- Unique support for portable and Smartphone devices
- Encrypted read and reply capabilities for all message recipients
- Secured compose capability for two-way communication
- Custom password policies tailored to your organization’s needs
- Innovative message and attachment compression
- Address book with support for group distribution
- Automatic generation of notifications and invitations

**ZixMobility™**

U.S. mobile users spend more time using e-mail on their phones than any other internet-based mobile activity. Yet, expectations of mobile users far surpassed existing technology in email encryption. Based on conventional, outdated email encryption standards, mobile email encryption users have struggled through rudimentary support, inconvenient steps, distorted layouts and cumbersome architectures. As a result, the power and benefits of secure email were severely stifled. ZixMobility addresses these challenges and elevates the standards for convenient secure email anytime, anywhere and on any mobile device.

A feature of ZixPort, ZixMobility enables business to stretch beyond conventional mobile limits by offering:

- Seamless email encryption as users navigate from desktop to mobile device
- Optimized layouts designed based on the user’s environment
- Fully functional navigation maximized for the user’s screen
- Maximum user convenience with no cumbersome steps
To ensure convenient delivery of secure email to your most valuable customers and business partners, ZixMobility is a standard ZixCorp feature, without any extra cost to ZixCorp customers.

**ZixMobility Key Features:**
- Seamless navigation between desktop and mobile device
- Screen layouts designed based on user device
- Maximized navigation based on user environment
- Extended email life of one year or more
- Functions across all internet-enabled mobile devices

**ZixMobility Benefits:**
- Convenient, secure email to your recipients through ZixPort at no extra cost
- Access to secure email without cumbersome steps
- No need to magnify and correct distorted layouts
- Improved productivity with real-time access to secure email

**ZixDirectSM**

*ZixDirect* is a delivery method that makes it possible to push an encrypted email directly to a user’s inbox. With *ZixDirect* there is no client software to install or maintain, and the user does not need to have any decryption capabilities to read the message. Users receive secure emails directly in their inbox and have the ability to read secure messages while working offline. An extension of our corporate wide *ZixGateway* service, *ZixDirect* makes it easier to choose the method of delivery that best meets the needs of the user.

**ZixDirect Key Benefits:**
- Secure messages sent directly to recipient’s email inbox
- Offline access to messages
- No additional software or training required
- Send-to-anyone capability
- Works seamlessly with existing systems
- Easy to deploy in under a day

**ZixDirect Key Features**
- Ability to recover messages if password is forgotten No pre-registration required
- Automatic retrieval and distribution of encryption keys
- Custom branding
- Secure read, reply and forward capability

**ZixConnectSM**

*ZixConnect* is a managed TLS service that allows companies to secure their email communication to multiple partners using a single TLS framework. *ZixConnect* is for organizations that need to secure email communications with key business partners, but are concerned about the long-term complexity of managing multiple separate TLS connections.
A single customer TLS connection to the ZixData Center can be all that is needed to secure emails communications to all partners. ZixCorp handles the set up and maintenance of each secure connection. ZixConnect is easy to set up and use. It deploys in just a few hours and is completely transparent to end-users.

Users send and receive messages that are encrypted in transit - no passwords, no hardware, and no software required. And, because the emails are in plain text within the corporate network, retention policies are maintained.

ZixConnect can also be used by existing ZixGateway customers that need to use TLS with certain business partners, but would rather not set up and maintain the TLS connection directly. ZixCorp works with the partners to set up TLS connections to the ZixData Center and then customers can send and receive emails through their ZixGateway appliance while their partners can send and receive using TLS.

ZixConnect Key Benefits:
- Secure email communications with key business partners
- No capital investment
- Deploys in just hours
- Transparent to end users
- No new customer hardware or software required

ZixConnect Key Features:
- Gateway design ensures email archiving compatibility
- Messages delivered to user in plain text
- Mandatory TLS ensures end-to-end security available

ZixDirectory
ZixDirectory is one of the largest email encryption directories in the world. It enables seamless and secure communication among its millions of members by providing a centralized directory for automated key exchange. As an added service provided with ZixGateway and ZixMail, the directory enables users to transparently send and receive encrypted emails without having to exchange certificates. In addition, when used with either ZixGateway or ZixMail, the directory makes it possible to send secure emails to anyone, anywhere, without pre-registration or configuration. By providing customers with an automated key management service, ZixCorp is able to greatly reduce the typical cost and complexity associated with email encryption solutions.

ZixDirectory Key Benefits:
- Access to email encryption directory
- Members include the federal banking regulators, state banking regulators and several departments of the U.S. Treasury
- Centralized and automated key exchange

ZixDirectory Key Features:
- Capacity, scalability, and infrastructure to support encryption keys for every email address in the world
- Public key validation and distribution in real time
- Transparent email encryption between ZixCorp users
• No key repository or PKI infrastructure to install or maintain
• Enterprise email encryption deployment in less than a day
• Reduced cost and improved ease-of-use for the organization
• High availability guaranteed through SLAs

ZixEnable℠
Leading healthcare, financial, government and insurance organizations have turned to ZixCorp to help them meet regulatory requirements and to protect customer privacy in their email communications. Now those organizations are leveraging email encryption as a strategic communication platform through ZixEnable.
ZixEnable is application-generated email encryption that enables businesses to secure the delivery of large-scale email communication containing personal private information. ZixEnable can be used to distribute personalized marketing campaigns, financial and health statements or other sensitive communication that businesses want sent in a timely and secure manner.

By using ZixEnable, businesses can experience:
• Improved customer loyalty by enabling highly personalized email communications while protecting sensitive customer information
• Increased cost savings and efficiencies by delivering sensitive information via email rather than paper mail
• Reduced risk of violating privacy regulations like HIPAA when delivering customer statements in email communications

To gauge the impact of ZixEnable, customers receive detailed summary reports on your application-generated email communication. Reports can be generated daily or weekly and include information such as what email was sent, who they were sent to and whether the email was read and when. In addition, a monthly summary report provides an overview of the effectiveness of your customer communication.

Customer Snapshot
Large health plan (LHP) delivers explanation of benefits (EoB) securely with ZixEnable.
• LHP member opts in
• LHP sets application to generate EoB emails
• Each EoB email is encrypted and placed in LHP's branded portal
• A notification email is sent to the covered member's email address
• The member opens the notification and clicks the "Open Message" button to view the EoB

• No key repository or PKI infrastructure to install or maintain
• Enterprise email encryption deployment in less than a day
• Reduced cost and improved ease-of-use for the organization
• High availability guaranteed through SLAs

ZixEnable℠
Leading healthcare, financial, government and insurance organizations have turned to ZixCorp to help them meet regulatory requirements and to protect customer privacy in their email communications. Now those organizations are leveraging email encryption as a strategic communication platform through ZixEnable.
ZixEnable is application-generated email encryption that enables businesses to secure the delivery of large-scale email communication containing personal private information. ZixEnable can be used to distribute personalized marketing campaigns, financial and health statements or other sensitive communication that businesses want sent in a timely and secure manner.

By using ZixEnable, businesses can experience:
• Improved customer loyalty by enabling highly personalized email communications while protecting sensitive customer information
• Increased cost savings and efficiencies by delivering sensitive information via email rather than paper mail
• Reduced risk of violating privacy regulations like HIPAA when delivering customer statements in email communications

To gauge the impact of ZixEnable, customers receive detailed summary reports on your application-generated email communication. Reports can be generated daily or weekly and include information such as what email was sent, who they were sent to and whether the email was read and when. In addition, a monthly summary report provides an overview of the effectiveness of your customer communication.

Customer Snapshot
Large health plan (LHP) delivers explanation of benefits (EoB) securely with ZixEnable.
• LHP member opts in
• LHP sets application to generate EoB emails
• Each EoB email is encrypted and placed in LHP's branded portal
• A notification email is sent to the covered member's email address
• The member opens the notification and clicks the "Open Message" button to view the EoB

12