

We Care for Your Security

At RBCConnex we understand that you're concerned about the security and privacy of your online transactions. This is why we use a robust Secure Socket Layer (SSL) certificate issued by **Let's Encrypt**, which is the Certificate Authority (CA) responsible for these certificates. Let's Encrypt ensures that all data transmitted between your browser and our server is encrypted and protected from unauthorized access, safeguarding sensitive information like login credentials and payment details."


Your computer and ours agree to transpose whatever we are sending into an unintelligible "hash" of characters, using a technology called SSL. For example: 3048 0241 00C9 18FA CF8D EB2D EFD5 FD37 89B9 E069 EA97 FC20 5E35 F577 EE31 C4FB C6E4 4811 7D86 BC8F BAFA 362F 922B F01B 2F40 C744 2654 C0DD 2881 D673 CA2B 4003 C266 E2CD CB02 0301 0001

Without the information on your computer or ours, no one can understand our encrypted communication.

For your safety, please expect anyone who communicates confidential information with you on the Internet to use encryption, the way we do.

What is SSL?

[Secure Sockets Layer, SSL](#), is the security technology for encrypting a link between a web server and a browser. All data passed between our web server and your browser remains private and secure.

Whenever you communicate with us on our website and payment pages, you will see a pad lock  on the upper left side of the page this is a sign that we are now engaging SSL.

How to know if an organization is real

To generate an encrypted SSL transmission, a web server requires an [SSL Certificate](#). Checking a website's certificate is good practice that helps you avoid spoof websites, sometimes called "phishing" sites. To check the certificate, click on the padlock. Your browser will show you the name of the owner of the certificate. This name should match the name of the website operator.

Our SSL certificates are issued by a leading certificate authority, Let's Encrypt Let's Encrypt is an automated, and open certificate authority (CA), run for the public's benefit. It is a service provided by the [Internet Security Research Group \(ISRG\)](#).

About Internet Security Research Group

ISRG's mission is to protect Internet users by lowering monetary, technological, and informational barriers to a more secure and privacy-respecting Internet.

ISRG was founded in May of 2013 to serve as a home for public-benefit digital infrastructure projects, the first of which was the [Let's Encrypt certificate authority](#). ISRG's founding directors were Josh Aas and Eric Rescorla. The group's founding sponsors and partners were Mozilla, the Electronic Frontier Foundation, the University of Michigan, Cisco, and Akamai.

In 2021, ISRG launched two new digital security projects: [Prossimo](#), a memory safety project, and [Divvi Up](#), a privacy-preserving metrics system.

Structure

ISRG is a California public benefit corporation, and is recognized by the IRS as a tax-exempt organization under Section 501(c)(3) of the Internal Revenue Code. Our EIN is 46-3344200.

Funding

ISRG is proudly sponsored by a diverse group of organizations, from small businesses and other non-profits to Fortune 100 companies. We aim to set an example for how everyone interested in a more secure Internet can work together to provide digital infrastructure for the public's benefit. See [this page](#) for more on our sponsors.

How do SSL certificates work?

How do SSL certificates work? An SSL certificate has the website's public key, as well as information specific to the site's identity. For transport layer security (TLS)/SSL **encryption** to work, devices trying to interface with the website need the site's public key, which identifies the server hosting the site. This is an essential element of the handshake that takes place when your browser connects with a site with TLS/SSL.

What is TLS? TLS is a protocol that uses **cryptography** to provide a secure connection between applications interacting with each other on the internet. It is a better version of SSL. Without the public key held within the SSL certificate, a TLS-secured connection cannot happen.

What Are The Elements Of An SSL Certificate?

An SSL certificate contains crucial information that serves to validate the certificate and associate it with the domain it is designed to help protect.

Domain name

The domain name refers to the name of the website, such as "Fortinet.com" or "Google.com." A certificate is issued for a specific domain name.

Name of the organization/individual to whom it is issued

This identifies the person or organization that either owns the website or helped set it up.

Issuing authority name

SSL certificates are issued by certificate authorities (CAs). They include the name of the authority that provided the certificate for the domain.

The certificate authority's digital signature

The digital signature of the CA ensures the authority listed as such in the SSL certificate is who they claim to be.

Associated subdomains

An SSL certificate can list subdomains associated with the primary domain. The subdomain comes before the primary domain in the address of a site. For example, in the address "docs.google.com," "docs" is the subdomain.

Date of issue

This indicates the date the SSL certificate was issued and associated with the domain and subdomains.

Expiration date

The expiration date tells you when the SSL certificate will expire. This is typically one to two years from the date of issue.

The public key

The public key consists of a string of numbers, letters, and characters used in the encryption and decryption of data sent between the site and users' browsers. The data encrypted by the public key can be decrypted using the private key.

Continuous Monitoring

To maintain the highest level of security, our SSL certificate is regularly monitored and updated to comply with the latest industry standards."