Soliton®

OneGate

Soliton OneGate is a service that delivers network level access and access to cloud applications using an X.509 certificate as the starting point for authentication. Everything an organisation would need to use X.509 certificates is built-in and easy to use.

The X.509 certificates are issued by an integrated certificate authority and deployed to remote clients with Soliton KeyManager. Network level access is provided by on-premises authentication components to LAN, Wi-Fi and VPN, and includes dynamic VLAN association to assign users to the VLAN they should be authorized to. Access to cloud applications is delivered through identity federation. Soliton OneGate (hereafter referred to as OneGate) is able to provision selected applications as well.

OneGate can completely remove the password from the logon process by replacing it with FIDO2 or an authenticator app. Combined X.509 certificate and FIDO2 / authenticator authentication will make two-factor log in not only a breeze but also more secure in the process. In case identity federation is not possible or FIDO2 login is not available, OneGate provides a built-in password manager that is able to retrieve complex password from the cloud service that can be used to authenticate, without the user having any knowledge on those passwords.

OneGate is provided as a managed cloud service, meaning every customer has its own private tenant that is not shared with other organisations.

How does it work?

OneGate integrates with existing user directories, such as on-premises Microsoft Active Directory or LDAP-servers or Microsoft Azure AD, but it is also possible to store user identities in the OneGate database itself if that is desirable.

To access OneGate, users need to request an X.509 certificate from OneGate first. They will do this using Soliton KeyManager, their logon credentials and a unique invitation code. Soliton KeyManager then ensures that the public and private key are generated on the client, that the public key of the certificate is transferred securely to OneGate, and that the necessary trust and X.509 client certificate are installed properly on the endpoint, removing this otherwise complex task from the user. Moreover, the Soliton KeyManager stays active in the background, alerting the user when the certificate is nearing its expiration date, allowing the user to renew the certificate in time. Because OneGate is a cloud service, Secure Key Manager can be used by both employees and people external to the organisation.

Once the certificate is in place, it can be used to securely access the company networks using a cable, the Wi-Fi or a VPN. In order to do this, OneGate uses one or more on-premises NetAttest EPS devices or virtual machines that integrate with the local network access servers. The authentication process is straightforward: when the user connects the first time, he/she will select the certificate to be used and after that access is provided seamlessly without any user intervention. If configured, the user will be authorized to the right VLAN at the same time - until the certificate is revoked or expires of course.

For Wi-Fi access there are additional benefits, because the so-called WPA Personal access using the well-known pre-shared key, that most companies use, does not provide much security. OneGate replaces this with WPA Enterprise, meaning that there is no longer need for multiple SSID's, MAC-address authentication and a password that is shared amongst all users. Once the OneGate client certificate is in place, users will be automatically and seamlessly connected to the correct VLAN when accessing Wi-Fi. With WPA Enterprise. security surpasses WPA Personal by using advanced encryption and individualized authentication, reducing intrusion risks.

In addition to providing network level access, OneGate has the ability to federate with cloud applications using SAML2. This means that when a user accesses the cloud application, he/she will be redirected to OneGate to log in. The user must then meet the application's authentication criteria, such as automatic certificate verification and being recognized by the Windows Hello camera, to gain access. This process is known as a Service Provider initiated login, where the user begins at their desired cloud application. OneGate also has a user portal displaying authorized applications. When accessed from this portal, OneGate facilitates entry by automatically verifying the certificate and performing a Windows Hello identification. For the user, this means a centralized and intuitive access point, which is more user-friendly than remembering URLs.

OneGate is able to provision a selected number of cloud applications . Provisioning user identities to cloud applications streamlines onboarding, enhances security, ensures consistent access controls, and improves overall user experience. Provisioning user identities is especially advantageous in scenarios with regular user additions and removals, ensuring swift, consistent, and secure access management. The use of short-lived certificates could complement the benefits of user provisioning, providing an added layer of security through automatic expiration.

If a user wants to access one of the company's cloud services, they will have to log in to OneGate first, using the X.509 client certificate as the starting point and providing (if required by policy) a second authentication factor. By default this is a password, but users can also register one or more FIDO2 security keys. FIDO2 security keys are typically USB devices, but could also use Bluetooth or NFC enabled devices, providing mobility. Alternatively, FIDO2 registrations like Windows Hello, integrated directly into specific hardware rather than relying on separate devices, can be set up to further simplify the login process. Using FIDO2 for authentication enhances account security by eliminating the vulnerability of exposed or guessable passwords.

If an application doesn't support federated access, a built-in password manager can be utilized; crucially, this solution stores passwords encrypted in the cloud, ensuring immediate availability across all of a user's devices, without retaining any local storage. In the scenario described, administrators can set usernames and passwords without the end user's awareness, streamlining the login process and enhancing security, thereby also safeguarding against phishing attacks and related threats.

Furthermore, OneGate incorporates policy and risk-based authentication, assessing factors like geo-location, to add another layer of precision and protection to the access management process.

The importance of two-factor mutual authentication

In today's connected world, making sure a client is who they say they are is paramount. It ensures that only legitimate users or systems can access sensitive data or functionalities, guarding against malicious intruders and potential breaches.

One of the most reliable ways to authenticate a client is through the use of an X.509 certificate. This certificate serves as a digital identity, issued and verified by a trusted Certificate Authority (CA), confirming that a client is indeed who it claims to be. Once both the client and server have presented their respective X.509 certificates, an mTLS (mutual Transport Layer Security) connection is established. This mTLS handshake ensures that both parties—client and server—are authenticated, resulting in a two-way, encrypted communication channel. Such a mutual authentication method, provided by mTLS, offers heightened security. Not only does it prevent unauthorized access, but it also protects against various sophisticated cyberattacks, such as man-in-the-middle schemes, ensuring a robust and secure digital environment.

User friendliness and security combined

OneGate provides each user a personal dashboard showing the applications they are authorized to, all in one place. This personal dashboard is only accessible after the browser has automatically provided the user certificate and (if required by policy) performed a second step, e.g. asking for a password or performing a Windows Hello authentication. From there, when users click on an application, OneGate handles the login behind the scenes.

OneGate allows setting the client certificate as a prerequisite to access the login page. The requirement of a client certificate on the IdP (Identity Provider) does significantly enhance security and acts as a deterrent against various attacks. For instance, automated bots and less-skilled attackers are blocked right at the start because they do not possess a valid client certificate. Also targeted attacks like password spraying or brute-force login attempts, are rendered ineffective if the attacker can't even reach the login page without a valid certificate.

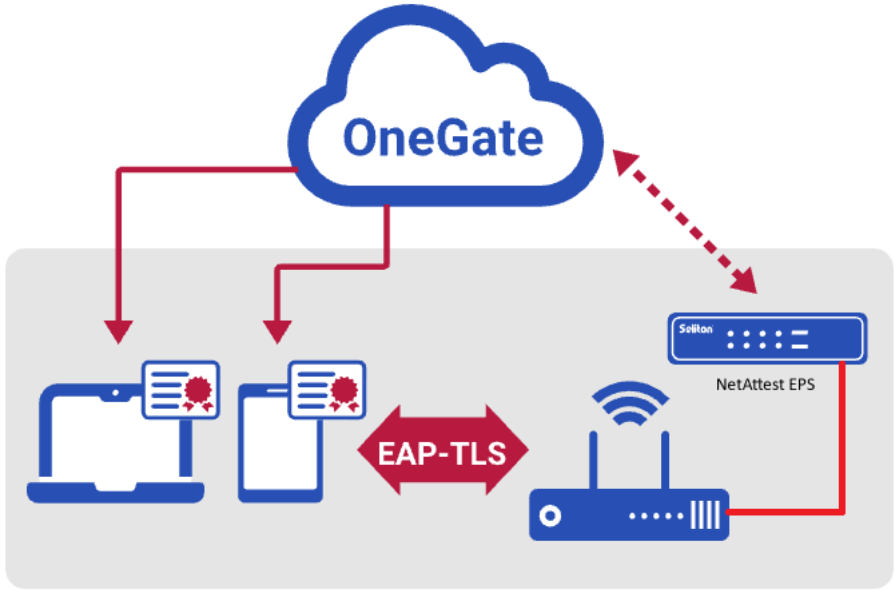
Our approach

OneGate strikes a delicate balance between offering robust security mechanisms and ensuring a frictionless user experience, making it a holistic choice for modern digital environments. This is achieved through:

- Enhanced Security: With the integration of two-factor mutual authentication, the solution ensures both the client and server validate each other's identities, using technologies like mTLS and X.509 certificates.
- Simplified User Experience: The user portal centralizes access to applications and facilitates secure single sign-on. Users won't need to remember multiple passwords, reducing the cognitive load.
- Robust Authentication Protocols: The solution's fallback to authenticator apps when FIDO2 is not available, coupled with the use of X.509 certificates, offers solid two-factor authentication.
- Automatic Access Restrictions: The system's ability to deny access when certificates expire or are revoked ensures that compromised or outdated credentials can't be used maliciously.
- Protection Against Targeted Attacks: By necessitating client certificates even before accessing the IdP login page, the solution deters and defends against targeted attacks, making it harder for attackers to initiate their assault.
- Versatility in Authentication: The option to use integrated hardware-based authentications like Windows Hello, instead of relying solely on separate hardware devices, offers flexibility in user verification.
- Comprehensive Logging and Oversight: Every interaction within the user portal is logged, facilitating oversight, compliance checks, and detailed audits.
- Policy and Risk-Based Authentication: By factoring in aspects like geolocation, the system can make more informed decisions about granting access, reducing the likelihood of unauthorized logins.
- Automated Convenience with Security: Through features like the built-in password manager, which stores credentials securely in the cloud, users are granted streamlined access without compromising security.
- Protection from Common Threats: By allowing administrators to set usernames and passwords without users' knowledge, the solution protects against phishing attacks and other threats that exploit user behaviour.

Key Features

- Two-Factor Mutual Authentication: Utilizes mTLS and X.509 certificates to ensure both sides in a communication session prove their identity to each other.
- User Portal: A centralized dashboard that provides users with easy access to both internal and cloud-based applications. It acts as the starting point for many users, streamlining their work process.
- FIDO2 authentication: The ability to use FIDO2 as a second-factor of authentication, rather than passwords, removing the risk commonly associated with passwords. This includes built-in solutions like Windows Hello, which are embedded in specific devices, and external hardware, such as FIDO2 enabled USB, Bluetooth or NFC-devices.
- Fallback Authenticator App: In scenarios where FIDO2 isn't an option, the system can still ensure robust two-factor authentication through a combination of X.509 certificates and an authenticator app.
- Secure Single Sign-On (SSO): Allows users to authenticate once and gain access to multiple applications without re-entering credentials, using SAML2 federation
- Built-in Password Manager: In case identity federation is not possible, offers secure storage of passwords in the cloud, not locally, with the added ability for administrators to set credentials unknown to the end user for added security.
- Automatic Access Control: The solution can automatically deny access if X.509 certificates expire or are revoked, enhancing security.
- Comprehensive Logging: All user interactions and activities within the portal are logged, facilitating audits and oversight.
- Policy and Risk-Based Authentication: Advanced authentication processes that factor in various risks, including geolocation, to determine access permissions.
- Client Certificate Requirement: Boosts security by requiring client certificates even before accessing the IdP login page, protecting against a range of threats, including targeted attacks.



EMEA office

Soliton Systems Europe N.V.

Barbara Strozzilaan 364 | 1083 HN
Amsterdam | The Netherlands

+31 (0)20 280 6060 |
emea@solitonsystems.com |
www.solitonsystems.com

Soliton®

Soliton Systems helps companies solve IT security challenges with a unique set of high quality, cost-effective products and solutions. As a global company with over 40 years of IT security experience, its solutions are deployed by many of the world's leading companies.