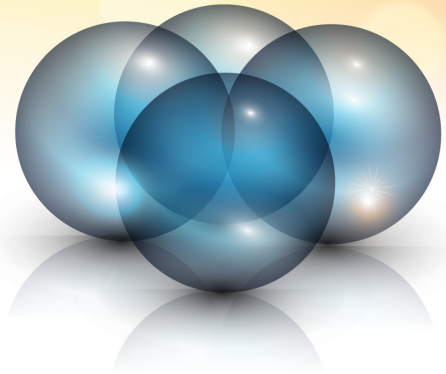

covisint | a Compuware Company

Cloud Authentication Services

Confirming User Identity at Login

Many authentication services are provided to confirm a user or computer identity before they access your systems. This service prevents unauthorized users from hacking into your systems. These services are provided for your users regardless of whether they are employees, contractors, suppliers, partners, clients or customers. This is done by directly binding the user to their credentials, and then providing him/her with a domain specific security token to be used for session security.

Cloud Authentication Services offers two-factor authentication and also provides support for identity risk scenarios at the time of authentication (Risk-based Authentication). Single factor authentication (SFA), which is standard, requires only a user ID and password. For a two-factor approach, a user simply enters a unique code along with their password to gain access to your system. If desired, two-factor authentication can be a mandatory requirement for your users each time they log into your system. When mandatory two-factor and risk-based authentication are combined, it is a very powerful tool to secure your systems. Covisint risk-based authentication can identify such scenarios as when your user is authenticating from an unknown device, location, outside of normal time parameters, and more.

The following two-factor authentication delivery mechanisms for one-time password codes are supported:

- **SMS Text** — a text message is sent to the user's registered phone number with the code to enter when challenged
- **Email** — a code is sent to the users email address
- **Phone Call** — A code appears on the screen that must be entered when the system calls the user's registered phone number
- **Mobile Push Notification** — Mobile login request sent to mobile device where user selects "approve" to acknowledge it
- **Smartphone Passcodes** — Passcode generated on mobile device and user enters it when challenged
- **IDcipher™** — the user is prompted to enter a code from an IDcipher card that has been provided to him by Covisint

Cloud Authentication Services include self-service features for changing a password, creating a new password if the user has forgotten their password, obtaining a forgotten user name, and additional management features for the other authenticators. Optionally, the user interface for the authentication service can display a link to a registration wizard, a link to check registration status, or provide a federated user with the ability to select their identity provider so that they can be redirected to the appropriate location for the authentication.

Risk-based Authentication

Risk-based authentication utilizes both user provided (e.g. username) and system collected user information (e.g. IP Address) to authenticate the user's request to the protected target resources. User provided data includes username and password, or SAML assertion for federated users. Collected user data includes attributes provided from internet communication

between the user and the authentication system (e.g. the user PC's IP address), as well as customer behavior and transaction patterns (e.g. login time and frequency). The collected information is used to evaluate the risk level of the access request. The risk level is evaluated against a set of pre-defined risk criteria and is used to decide if two-factor authentication is needed.

Risk-based authentication assessments occur at initial login or federation and may also be performed each time the user requests access to resources or conducts transactions that require a higher level of protection. The following criteria will be used to determine the risk of a specific authentication activity:

- Name of Identity Provider
- Computer or device recognition (from previous session)
- Any IP address or IP subnet not identified and provided by customer is considered high risk
- Specific times of day, depending on local time zone
- Time lapse between last access and current request
- Frequency of access
- Repetitiveness of access
- First-time login is always a higher risk

IDcipher™ Card Authentication

The IDcipher Card Authentication is a low-cost, easy-to-use, easy-to-deploy authentication mechanism that provides an extra layer of assurance for users to authenticate to a secured system. In this method, the user, after presenting a valid user ID and password, is prompted to enter a value from an IDcipher card that has been provided to him by Covisint via email. This method of authentication allows for a two-factor access method without needing to manage a hardware token.

The IDcipher card is an 8x8 matrix, where each cell contains the value of a randomly generated four-character lower-case alphanumeric string (number "0" and letter "o" are excluded). The card will be emailed to the user in PDF format. The user will print out a hard copy of the card, which is the physical size of a credit card. At authentication time, the IDcipher Card system challenges the user for the value of a randomly selected cell. The user enters the value read from their IDcipher Card, it is validated by the IDcipher Card system, and, if correct, the user's authentication request is successfully completed.

For more information, go to identity.covisint.com today.

Covisint World Headquarters
One Campus Martius
Detroit, Michigan 48226
United States of America
888.222.1700 phone
www.covisint.com