Soliton

G/On

It’s G/On - only even more flexible

Authenticate user access to remote applications on a zero trust basis, with all the flexibility your customers’ needs.

Authenticating users ensures the right people have access to the right tools at the right time. But what happens when authentication methods don’t work or aren’t right for an organisation?

It’s a problem many organisations face. But the answer is clear: introduce a flexible relationship between authentication and authorisation, which means you can now use multiple authentication factors to determine the authorisation level.

G/On 7.2 opens up options to use external authentication, including services like Google authenticator or the Duo app. These can be used instead of or combined with G/On’s authentication factors, creating a lot of possibilities to improve the service level to the user.

Never worry again about what happens if a token breaks, gets lost or is forgotten, and users aren’t able to gain access. Instead, embrace a new, flexible approach to authentication, keeping people working and maintaining the security levels your customers need.

Set the rules you need

For specific applications or data, set rules requiring a certain level of assurance, for instance, mandating that users need to have a smart card for highly sensitive data. But for other services or data that don’t require the same high levels of authentication, alternative rules can be in place — for example, username and password on a business computer or username and password with authentication using a phone.

Unlocking zero trust solutions in new markets

Using a security token is, of course, the highest level of authentication available. However, there are cases when the number of users or the type of applications means it isn't considered worth the financial investment - and, in the past, this would be where the conversation would end.

Some user groups cannot be serviced with authentication tokens—for example, smart cards—because it's not cost-effective. If your customer has many users, maybe not even limited to employees, it's not practical to purchase all the tokens needed. By supporting external authentication factors, it opens up G/On to new potential user groups. And for markets where it's too difficult to handle the logistics for physical tokens, flexible authentication overcomes this hurdle.

G/On is now accessible to a wider range of companies. The flexible authentication allows you to set up systems for customers with way more granular access and offer way more flexibility in setting it up for users, helping your customers.

Keep people working

The application with the highest risk profile determines the authentication level needed. For highly secure applications, access may only be possible with the security token. But for other applications that don't require such high levels of security, users can use other means of authentication.

When users cannot work because they cannot get access, it's frustrating and costly. Whether their token isn't working or they've not even received it, the solution is hindering rather than helping them in these cases.

Flexible authentication schemes mean users can still be granted access to some applications where they do not need the same level of security. It won't enable access to the most secure application, but it means they can continue working.

G/On is and always has been a zero trust solution. It's always determined user authorisation based on high levels of authentication, and it's just now even more flexible to make this happen in a way to suit your customers.

Soliton Systems Europe N.V. | Barbara Strozzilaan 364, 1083 HN Amsterdam, The Netherlands
+31 (0)20 896 5841 | emea@solitonsystems.com | www.solitonsystems.com