# It's G/On - only even more flexible

Authenticate user access to remote applications on a zero trust basis with all the flexibility you need.

**Authenticating users ensures the right people can access the right tools at the right time. But what happens when authentication methods don't work or aren't right for an organisation? Often, organisations need help providing appropriate access to their various users who require different levels of authentication, which results in security risks or access restrictions that hinder productivity.**

This is a problem many organisations need help with. But the answer is clear: introduce a flexible relationship between authentication and authorisation. With this approach, you can now use multiple authentication factors to determine the authorisation level providing greater security and ease of access.

G/On 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. Using flexible authentication allows you to set up a system that caters to your diverse user vase enabling you to provide the right level of access at the right time.

Never worry again about what happens if a token breaks, gets lost or is forgotten, and users can't 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, such as mandating that users need 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

G/On serves various end-user use cases requiring remote access. While a security token provides the highest level of authentication available, it may only sometimes be practical for some organisations due to the number of users or the type of applications. For instance, purchasing smart cards can be expensive and unsuitable for certain user groups, such as third-party users requiring access to some of your resources. In addition, G/On's flexible authentication can overcome the challenge of managing physical tokens in markets where it isn't easy to overlook the logistics of physical tokens.

G/On caters to a broader range of companies, enabling more granular access and greater flexibility in user authentication. Whether you have a small team or a large user base, G/On can assist you in providing zero trust access to the right people at the right time. With G/On, you can choose the appropriate level of authentication based on the user and situation, ensuring that security is not compromised. G/On offers a range of authentication factors that adapt to various use cases, allowing you to balance user convenience and strong security measures. Whether you have numerous users or require an alternative authentication method, G/On has you covered.

## 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, 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 still need to receive 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 now even more flexible to make this happen to suit your customers.