



Gemalto Explains
**Strong Authentication
for Cloud Computing**



How it works

OTP-based Strong Authentication for Cloud Computing

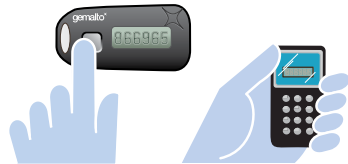
1

Local or remote user is prompted to create a **one-time password (OTP)** for authentication to cloud service.



2

User **creates an OTP** by pushing a button on his OTP device, or by using a mobile application to generate the OTP.



3

The OTP appears on the device screen or mobile phone, and **the user enters it along with his username.**



4

The **cloud service verifies the username and OTP** and **the user is securely authenticated** to the cloud service.



How does this make cloud computing secure?

45
67890
1234
6789

- OTP's offering strong, two-factor authentication, using something you "know" (your username) and something you "have" (your OTP device or mobile phone)

866965

- The OTP is unique to this session and cannot be used again

???

- OTP's offer strong security because they cannot be guessed or hacked

Benefits:



- Provides protection from unauthorized access



- Easier to use for the employee than complex frequently changing passwords



- Easy to deploy for the administrator



- Is a good first step to strong authentication in an organization

= Higher cloud security with more convenience.

How it works

Strong authentication technology

Benefits of OTP technology:

- Low cost way to deploy strong authentication
- Simple integration with existing infrastructure
- Easy to deploy and manage
- Allows easy upgrade to PKI-based authentication in the future

Gemalto Strong OTP Authentication fits many types of organizations:



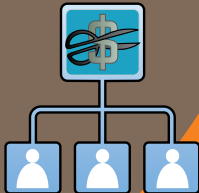
Cloud service providers

Add essential strong authentication to your web services



Online gaming providers

Secure gamers' access to their accounts



Small & medium-size businesses

Deploy strong authentication easily and at low cost



Enterprises

Meet regulatory requirements and improve password management