DigitaleFacile

La tua guida al digitale

4. Privacy e Sicurezza

4.3

La strong authentication

Finanziato dall'Unione europea NextGenerationEU
REPUBBLICA DIGITALE
DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE
Regione Lombardia
PUNTO DIGITALE FACILE

La strong authentication

Cosa è?

L'Autenticazione forte del Cliente (dall'inglese Strong Customer Authentication o SCA) è una misura di protezione degli *account* personali che richiede due o tre fattori di riconoscimento.

Si tratta di un sistema che risponde a specifici requisiti. Per *l'autenticazione a due fattori* questi sono: conoscenza (una *password* personale) e possesso (generalmente un dispositivo elettronico come uno *smartphone* sul quale possono essere inviati codici temporanei).
Per quella a tre fattori, oltre a quelli sopracitati, c'è in più il requisito dell'*inerenza*, come l'impronta digitale o il riconoscimento facciale.

Precise normative dell'Unione Europea regolamentano gli ambiti in cui l'autenticazione forte del cliente è obbligatoria e quelli in cui invece non è richiesta. È tuttavia lasciata ai singoli fornitori dei servizi online la facoltà di applicarla sui propri sistemi.

A cosa serve?

Il riconoscimento a due fattori è il sistema attualmente più utilizzato per proteggere i dati personali nei servizi online.

È obbligatorio per accedere a siti e applicazioni che necessitano di un alto grado di protezione, come ad esempio quelli bancari e assicurativi, ma è sempre più utilizzato anche in altri ambiti per prevenire e contrastare gli attacchi di *virus informatici*.

Come si fa per...

...attivarla

Le persone non possono chiedere a un fornitore di servizi online di attivare il servizio di riconoscimento a due o tre fattori.

Viceversa, è il fornitore dei servizi online a chiedere ai clienti di essere autenticati tramite questo sistema di riconoscimento.

...usarla

Dopo essersi registrato al sito di interesse (ad esempio quello della propria banca) con le sue *credenziali di autenticazione (username e password*), l'utente può scegliere in che modo e su quale dispositivo ricevere il *codice temporaneo (OTP*) che rappresenta il secondo fattore di autenticazione.

In alcuni casi il codice viene inviato per messaggio *SMS*, altre volte per mezzo di applicazioni sicure (*soft token*) che generano automaticamente i codici temporanei e li rendono disponibili per pochi secondi. Altri sistemi ancora richiedono la lettura di un *QR Code* che deve essere inquadrato dalla fotocamera dello smartphone per abilitare il riconoscimento.

Il codice temporaneo OTP, a sei cifre, va introdotto negli spazi indicati dal sistema che, riconosciutolo, sblocca l'accesso al sito.

Nel caso di autenticazione a tre fattori è richiesto un ulteriore sistema di sicurezza, generalmente l'impronta digitale o il riconoscimento facciale.

La strong authentication

Fai sempre attenzione a...

Come per tutti i servizi online che richiedono l'immissione di dati, è importante seguire alcune semplici ma fondamentali regole di sicurezza.

Custodire sempre con cura le password e non fornire per nessun motivo le proprie credenziali di accesso ai servizi bancari (specie se richieste via e-mail o con un messaggio).

Controllare allegati e *link* inviati per posta elettronica e non usare *connessioni pubbliche* che non prevedano l'inserimento di una password.

Installare solo applicazioni verificate e tenere attivo il *software antivirus* sui propri dispositivi elettronici.

Alcuni siti prevedono, in fase di attivazione della SCA, una "chiave di recupero" da conservare con la massima cura. Questo codice è infatti indispensabile in caso di dimenticanza, furto o smarrimento della password per sbloccare il sistema e ripristinare le proprie credenziali.

Da sapere...

Attualmente, l'autenticazione forte del Cliente a due fattori è il più diffuso sistema di protezione dei dati personali.
Anche lo *SPID (Sistema Pubblico di Identità Digitale),* che consente l'accesso ai servizi dell'Amministrazione Pubblica, prevede il riconoscimento a due fattori.

Esistono diverse *applicazioni* gratuite che consentono la creazione dei codici temporanei OTP (ad esempio Google Authenticator o Microsoft Authenticator) e sono numerosi i *gestori di servizi internet* che hanno sviluppato sistemi di soft token da scaricare sul proprio smartphone e che generano codici sicuri.

La legge indica i casi in cui non è richiesta l'autenticazione forte del cliente come, ad esempio, per l'accesso alle sole informazioni sui conti online, per pagamenti online di importi non superiori a 30 euro, pagamenti ricorrenti allo stesso beneficiario (e dello stesso importo), giroconti e altri piccoli pagamenti per determinati servizi (es. parcheggi o trasporti).

La strong authentication

GLOSSARIO

ACCOUNT – È l'insieme dei dati identificativi che consentono l'accesso di un utente a un determinato servizio online. Tali dati (nome, password, e-mail ecc...) sono depositati presso il gestore del servizio e consentono il riconoscimento dell'utente.

ANTIVIRUS – Programma informatico che, in base a diversi livelli di protezione, rileva, blocca e rimuove virus da strumenti elettronici collegati alla rete internet.

APPLICAZIONI – Abbreviate spesso con "APP", sono un programmi creati per essere installati e utilizzati sui dispositivi mobili.

AUTENTICAZIONE A DUE FATTORI – Metodo di riconoscimento sicuro degli accessi che prevede l'uso di due sistemi di identificazione (ad esempio, password e codice OTP).

CODICE TEMPORANEO (OTP) – Password temporanea generata da appositi dispositivi necessaria in caso di autenticazione di secondo livello. È generata da appositi dispositivi e inviata all'utente tramite SMS, e-mail o applicazioni per smartphone.

CONNESSIONE PUBBLICA – Collegamento a una rete internet a libero accesso e non protetto da password o altro sistema di sicurezza.

CREDENZIALI DI AUTENTICAZIONE (O ACCESSO) – Generalmente costituite dal nome utente e dalla password. Consentono l'ingresso a siti / servizi.

GESTORI DI SERVIZI INTERNET – Chiamati anche Provider, Società che consentono ai propri utenti l'uso della rete internet e dei servizi connessi. Dall'inglese Internet Service Providers (ISP).

INERENZA – Stretta connessione fra due cose che sono inscindibili (ad esempio, l'impronta digitale o i lineamenti del volto di un soggetto.

LINK – Abbreviazione di hyperlink, o collegamento ipertestuale. È una parola, frase o immagine che, una volta selezionata, apre altre pagine o siti internet.

PASSWORD – Parola d'ordine composta da caratteri alfabetici, numerici e simboli, creata per proteggere l'accesso a computer e servizi digitali.

QR CODE – Codice grafico che racchiude dati e informazioni. Inquadrandolo con la fotocamera dello smartphone apre la pagina internet che le contiene.

SMARTPHONE – Significa "telefono intelligente". Grazie al sistema operativo unisce le caratteristiche di un telefono con quelle di un computer.

SMS – Breve messaggio di testo scambiato in tempo reale fra due o più soggetti che utilizzano dispositivi elettronici connessi alla rete (computer, tablet, smartphone).

La strong authentication

SOFT TOKEN – Applicazione che consente la creazione di codici temporanei OTP. È installato direttamente sul dispositivo elettronico dell'utente.

SPID (SISTEMA PUBBLICO DI IDENTITÀ DIGITALE) – Forma di riconoscimento dell'identità personale che funziona grazie all'utilizzo di un codice utente e di una password.

USERNAME – Anche detto "nome utente", è parte con la password delle credenziali d'accesso.

VIRUS INFORMATICO – Programma che si installa in modo involontario sugli strumenti elettronici causando perdita di dati e danneggiamento dei sistemi.

Per maggiori informazioni

Per maggiori informazioni sull'autenticazione forte del Cliente e le modalità di attivazione e utilizzo, rivolgersi ai facilitatori regionali.

www.regione.lombardia.it