# MODALITA' DI ACCESSO
## AGLI IMPIANTI E AI SERVIZI

L'accesso agli impianti e ai servizi avviene esclusivamente tramite apposito bracciale smart card, che consente, tramite codice identificativo univoco la verifica dell'identità personale e delle relative abilitazioni associative, assicurative e sanitarie dell'utente. Il bracciale viene consegnato gratuitamente in sede di primo tesseramento e rimane di proprietà del tesserato.

Qualora l'utente acconsenta esplicitamente alla rilevazione dell'impronta digitale, il dato biometrico verrà convertito in un codice numerico e conservato esclusivamente nel bracciale, che consentirà **l'accesso diretto, automatizzato, agli impianti e ai servizi (apertura dei tornelli)**.

Qualora invece l'utente non desideri che l'impronta digitale sia rilevata, dovrà presentare al personale di segreteria ad ogni accesso **un documento d'identità in corso di validità**. Una volta effettuato il riconoscimento il personale abiliterà il braccialetto per l'accesso.

In assenza del bracciale non è possibile l'accesso agli impianti e ai servizi. In caso di smarrimento o danneggiamento il bracciale può essere sostituito al costo di Euro 5.

### PRECISAZIONI SUL PROCEDIMENTO DI RILEVAZIONE DI IMPRONTA DIGITALE

Si applica il Provvedimento Generale Prescrittivo in tema di biometria del Garante per la Protezione dei Dati Personali n. 513 del 12.11.2014 per quanto riguarda l'uso dell'impronta digitale a scopi facilitativi per cui è garantito il rispetto delle seguenti prescrizioni:

a) Le caratteristiche biometriche consistono nell'impronta digitale.
b) La cancellazione dei dati biometrici grezzi e dei campioni biometrici ha luogo immediatamente dopo la loro raccolta e trasformazione in modelli biometrici.
c) I dispositivi per l'acquisizione iniziale e quelli per l'acquisizione nel corso dell'ordinario funzionamento sono direttamente connessi o integrati, rispettivamente, nelle postazioni informatiche di enrolment e nelle postazioni di controllo o nei dispositivi di acquisizione.
d) Le trasmissioni di dati tra i dispositivi di acquisizione e le altre componenti del sistema biometrico sono rese sicure con l'ausilio di tecniche crittografiche con lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita dei dati.
e) Si applica l'esclusiva conservazione del riferimento biometrico in modalità sicura su supporti portatili (bracciale smart card) dotati di adeguate capacità crittografiche e certificati per la funzionalità richiesta in conformità alla norma tecnica UNI CEI ISO/IEC 15408 o FIPS 140-2 almeno level 3:
    i. il supporto è rilasciano in un unico esemplare ed è nell'esclusiva disponibilità dell'interessato;
    ii. l'area di memoria in cui sono conservati i riferimenti biometrici è accessibile ai soli lettori autorizzati ed è protetta da accessi non autorizzati;
    iii. il riferimento biometrico è cifrato con tecniche crittografiche con lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita dei dati.
f) Non viene applicata la conservazione del riferimento biometrico su un dispositivo-lettore o su postazioni informatiche.
g) E' esclusa la realizzazione di archivi biometrici centralizzati.