NTT DATA
Trusted Global Innovator

Codename BaBeLe: Dati biometrici e crittografia omomorfica

16 Ottobre 2019

Sala del Consiglio Provinciale, Perugia

De Componendis Cifris

NTT Group

SOLUTIONS AND APPLICATIONS

NTT DATA

50+ countries
110K professionals

TELECOMMUNICATIONS CARRIER

docomo
NTT EAST
NTT WEST

MANAGED ICT & DATA CENTER NETWORK

dimension data
NTT Security
NTT Communications

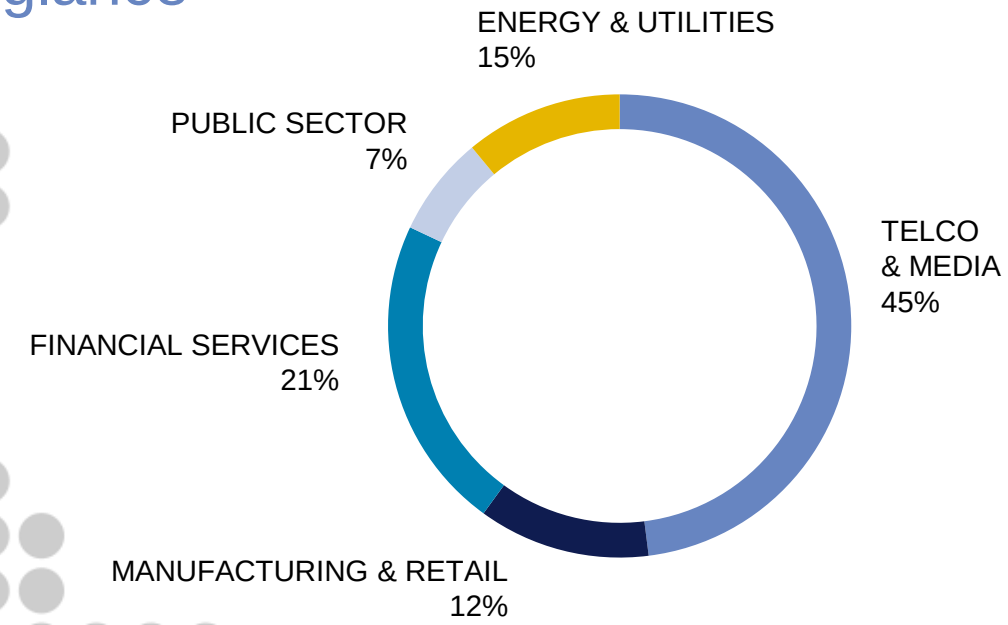
NTT

100+ countries
275K professionals

INNOVATION

NTT R&D
NTT INNOVATION INSTITUTE, INC.

NTT DATA Italia at a glance



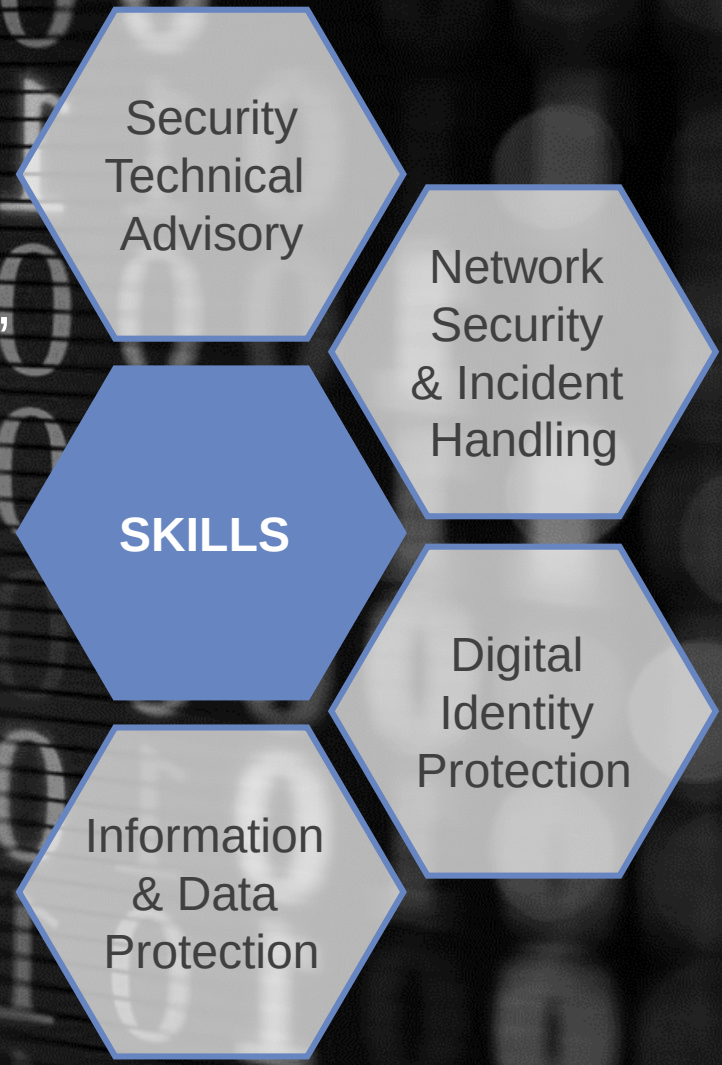
8 headquarters

~3300 professionals

- CONSULTING
- DIGITAL
- **SECURITY**
- SYSTEM INTEGRATION
- NETWORK
- BUSINESS INTELLIGENCE
- MOBILE
- MANAGED SERVICES

Cyber Security @ NTT DATA Italia

- ✓ Active since 2001
- ✓ End-to-end offering, from consulting to **ethical hacking**, from managed services to security solutions delivery
- ✓ More than 450 high-skilled professionals
- ✓ Partnership with main security technologies suppliers
- ✓ Primary references in every market sectors
- ✓ Strong links with universities and R&D centers



Our commitment in R&D and Innovation

INVESTING

$4

BILLION

ANNUALLY

R&D STAFF

6,000

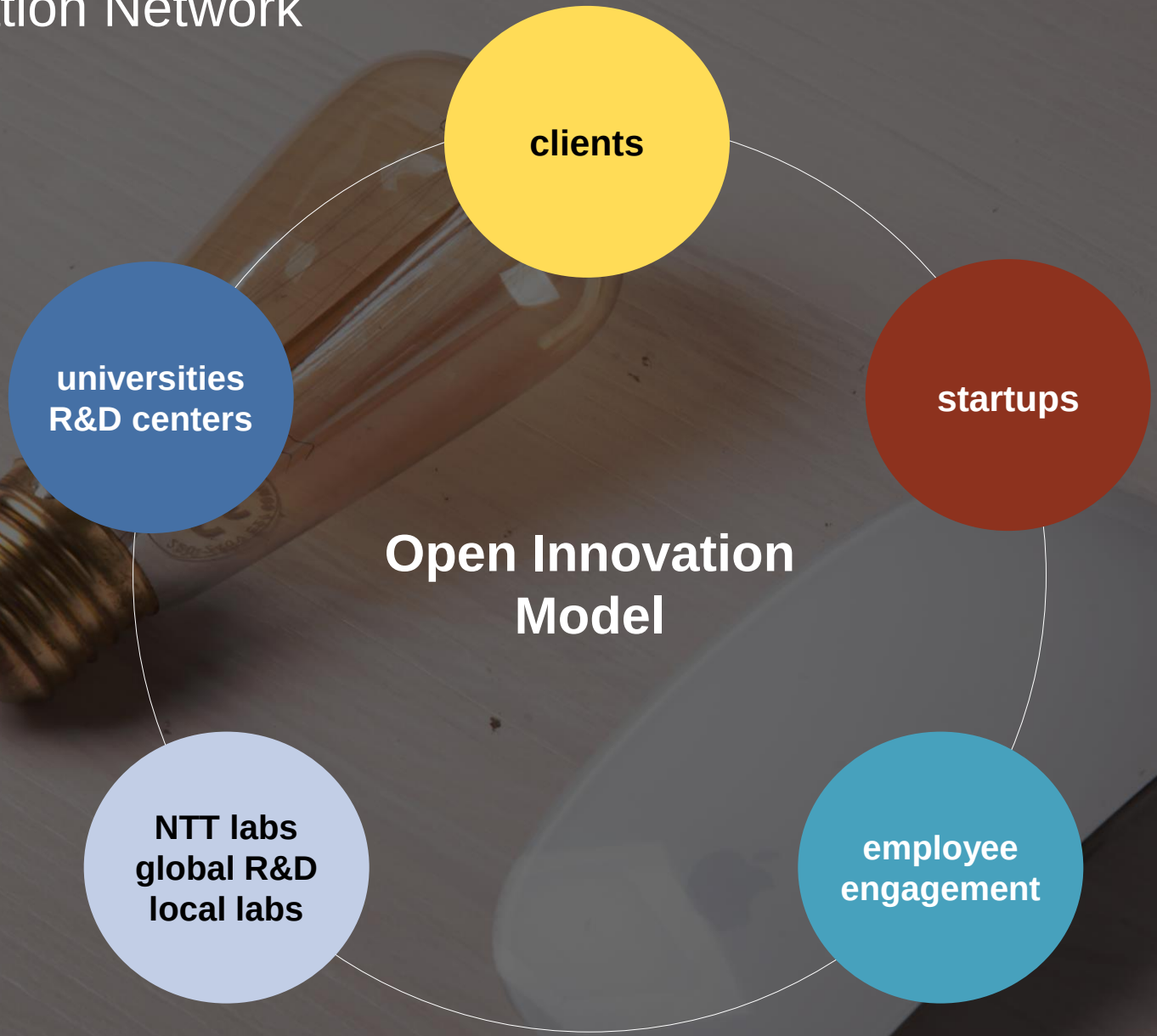
PALO ALTO

COSENZA

TOKYO

NTT DATA

NTT DATA Innovation Network



NTT DATA

Baccarelli

Raffaele.Baccarelli@nttdata.com

Benucci

Alessandra.Benucci@nttdata.com

Leccese

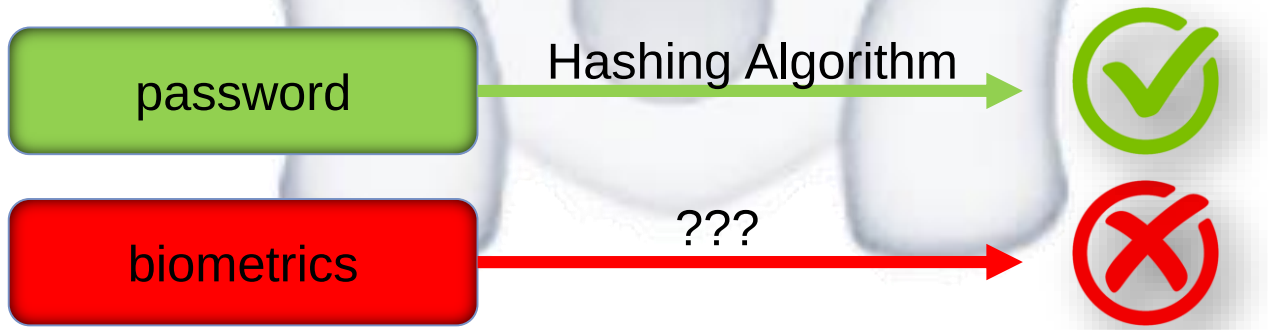
Francesco.Leccese@nttdata.com

A fingerprint-based secure authentication protocol

NTT DATA

L’importanza del dato biometrico

- ✓ Il 25 Maggio 2018 entra in vigore il **General Data Protection Regulation**, Regolamento dell'Unione Europea in materia di dati personali e privacy
- ✓ Il legislatore europeo ha riservato al dato biometrico una rilevanza specifica all’interno della generale categoria dei dati sensibili (*Art. 9*)
- ✓ Ciò è confermato dalla previsione contenuta nel GDPR di una disciplina particolarmente tutelante e fondata su una serie di adempimenti obbligatori (*Artt. 30, 35*)
- ✓ Vi è dunque la necessità di proteggere adeguatamente la confidenzialità del dato biometrico, in particolare per le finalità di riconoscimento/autenticazione



Una possibile soluzione: la Crittografia Omomorfica

Moderne tecniche di cifratura che consentono di ottenere determinate informazioni sui messaggi dalla **sola manpolazione delle loro cifrature**

Esempio RSA: $Siano\ p,q \in \mathbb{N}\ primi, N = pq, e\ \phi(N) = (p-1)(q-1);\ \ e,d \in \mathbb{N}\ t.c.\ GCD(\phi(N),e) \equiv 1\ e\ t.c.\ ed \equiv 1\ mod\ \phi(N);\ Dato\ un\ messaggio\ in\ chiaro\ m \in \mathbb{N}, si\ pone:$

$$enc_e(m) = m^e\ mod\ N = c;\quad dec_d(c) = c^d\ mod\ N = m^{ed}\ mod\ N = m;$$

Magic trick!

$$\boldsymbol{enc_e(m_1) * enc_e(m_2)} = m_1^e * m_2^e = (m_1 * m_2)^e = \boldsymbol{enc_e(m_1 * m_2)}$$

L'idea alla base del protocollo **BaBeLe** prevede l'utilizzo di un **crittosistema omomorfico** finalizzato ad individuare una procedura che simuli *de facto* un algoritmo di hashing che possa poi esser applicato ad un dato biometrico e conseguentemente abilitare un effettivo **protocollo di autenticazione** sicuro basato su dati biometrici.

Il caso di studio: le impronte digitali

Nell'ambito dell'autenticazione, un'impronta digitale non è altro che l'insieme di bordi e valli che generano forme e disegni arbitrari.

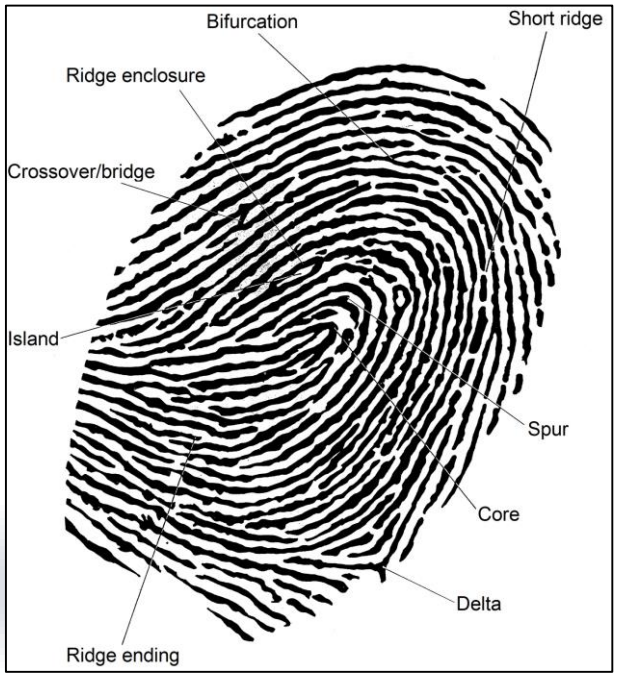
L'idea: Determinare un metodo per riconoscere e classificare le *minutiae* di un'impronta, cioè gli schemi più comuni e frequenti.

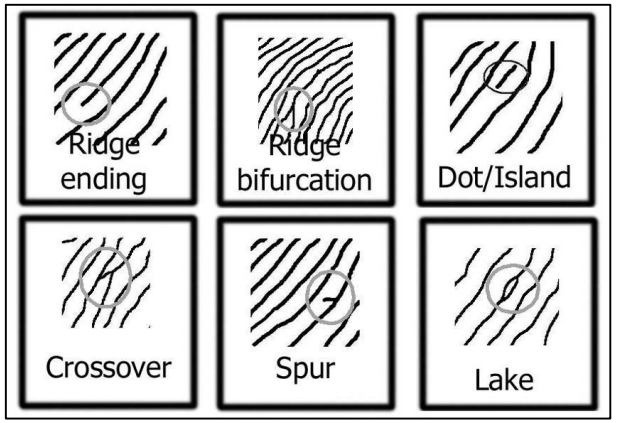
Una *minutia* viene rappresentata in una quintupla del tipo

$$\mathrm{m} = (t, x, y, \theta, \rho)$$

Si definisce il *template di un'impronta digitale* come

$$\mathcal{T} = \{(t_i, x_i, y_i, \theta_i, \rho_i)_{i \in I}\}$$





Dalla scansione ai numeri

Scansione di un'impronta digitale proveniente da uno scanner comune

Esempio di minutiae estratte dalla scansione attraverso il software MINDTCT [1]

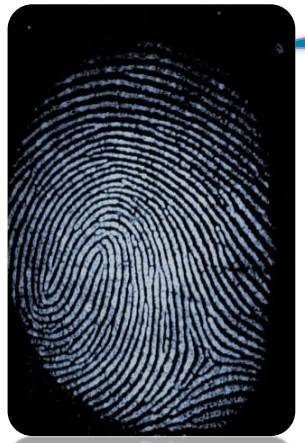
M1 = [0, 34, 302, 3, .427]
M2 = [0, 47, 235, 5, .8]
M3 = [0, 54, 222, 5, .353]
M4 = [0, 61, 208, 5, .398]
M5 = [0, 61, 367, 17, .224]
M6 = [0, 76, 344, 17, .263]
M7 = [0, 81, 281, 20, .638]
M8 = [0, 84, 380, 17, .117]
M9 = [0, 105, 353, 17, .232]
M10 = [0, 106, 222, 23, .714]

$\mathbf{t}_1$=[X:x5cb0fc3ab4e0dd36810a481fca18a18eb3d8695b78d734d55caefd313205369a;Y:0x3c5ae067e27cd9bcc48ec02429697a9443b797163906d6fdea3a4b180e7c3f18][X:0x5a923633d31c2dfa87e1cb6628f58c548582cfdf46dc520172c65ccef26822a9;Y:0xdce302eb6d83543d5ef03a81448cd3528ff565d8080c14985cd714ed66d07514]),
$\mathbf{x}_1$=[X:0x9a2061ad8cd9b14979a57742bf1ff652f3dc83032830dcd047fbe7a23758c9eb;Y:0x1c043928b2078e38b45246b564aa8899295108d1c7e5bf6590c9c634e5a7a30c][X:0x5b7d618e8b2446c49a8a9da001e7eade4cd4f4d253c38cc952f193e5bcc205a7;Y:0x54b2208e487db877cc9f8f2e3087580ae612a4c489949af6daa2eb72e65d8b59]),
$\mathbf{y}_1$=[X:x65f9e9563586c0d804d4155386c6e78204ba5e5f138aeaaf86816b69228105c0;Y:0xfe096130dc957910b2c13205bc397fcfb138fcaedfc23b32e8a4baa970f652fc][X:0x1b7fe58e5c13d3aaf1226fa46c503d3d37da7a720547fc4ea512ac7e11139ccd;Y:0xb72f789362ac4e518a9371543803928d47dca22cb3c32861439babb34da70002]),
$\boldsymbol{\theta}_1$=([X:xa568759e8d35d5e3c49b26055e6681fb72831f744f7c35f9c0df5ef0741483a9;Y:0x336a95f2b87d8f6d0630d41c8b47f44da6dc911ed72f1bf211dfc8d04b05d539][X:0xce804ebb54b2170a2fc00d16b4d8e0b8d08d1b2f64fa6c4fefed1a03a4035968;Y:x52b56c02da8abea6258fe8e2a51bf78ad5d34fe989e089816086a145976edf2d])

Minutia cifrata con il crittosistema omomorfico
In questo caso un crittosistema basato sulle curve ellittiche.

[1] https://www.nist.gov/services-resources/software/nist-biometric-image-software-nbis

Dai numeri all'autenticazione



$enc_k(C_1)$
$enc_k(C_2)$
$enc_k(C_3)$
…

$enc_k(C_1) \oplus enc_k(P_1)$
$enc_k(C_2) \oplus enc_k(P_2)$
$enc_k(C_3) \oplus enc_k(P_3)$
…

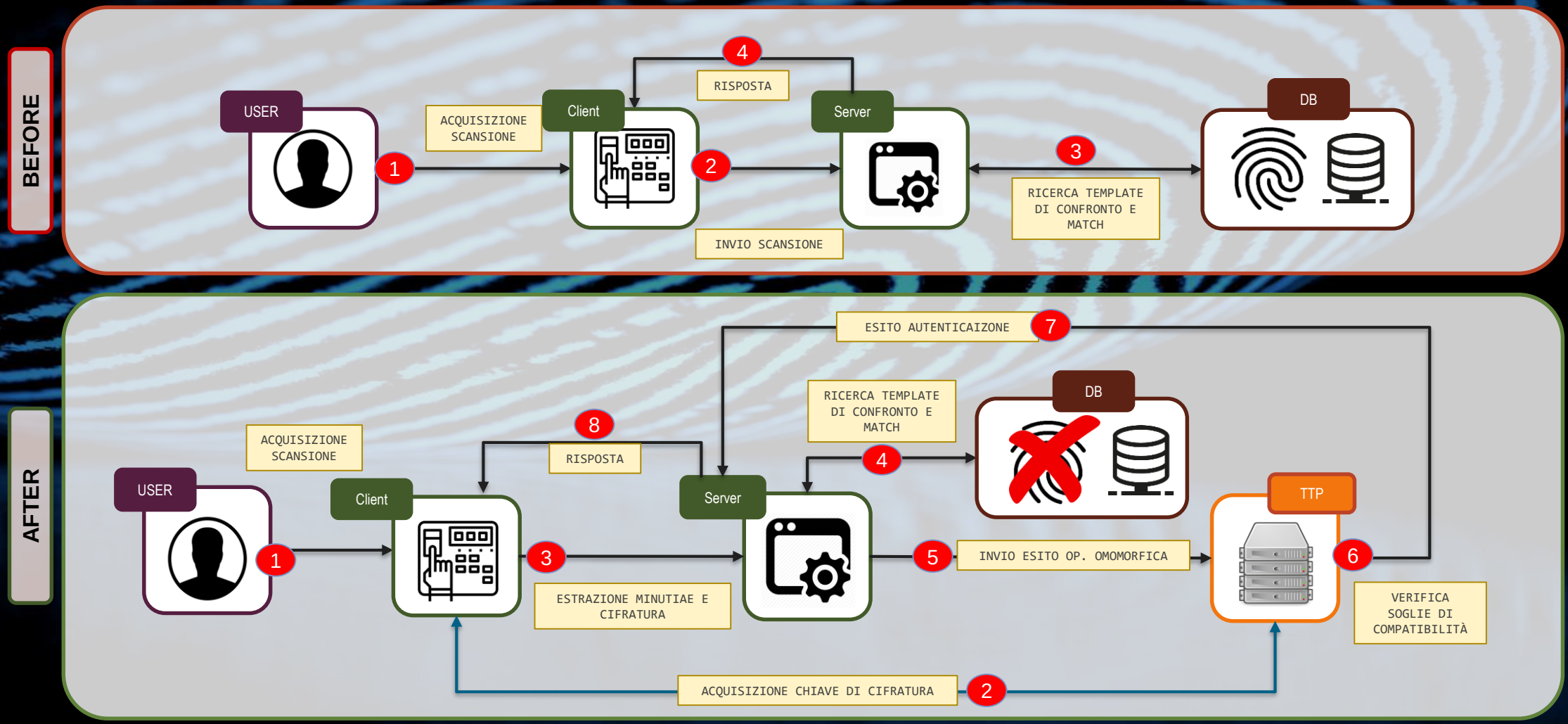
$enc_k(P_1)$
$enc_k(P_2)$
$enc_k(P_3)$
…

$$enc_k(C_i) \oplus enc_k(P_j) \xrightarrow{Decrypt_k} \Delta_{ij} = (\tilde{t}, \tilde{x}, \tilde{y}, \tilde{\theta}, \tilde{\rho})$$

$$match(C_i, P_j) = \begin{cases} ok & \text{se } \Delta_{ij} \leq \varepsilon \\ ko & \text{se } \Delta_{ij} > \varepsilon \end{cases}$$

Dove $\varepsilon = (\varepsilon_t, \varepsilon_x, \varepsilon_y, \varepsilon_\theta, \varepsilon_\rho)$ rappresenta un vettore di soglie prestabilito. Ogni Δ_{ij} rappresenta il valore della **compatibilità** tra le *minutiae* C_i e P_j.
L'esito del match di due template è determinato dal **numero di coppie di *minutiae*** che sono ritenute compatibili.

BaBeLe authentication protocol



BaBeLe dream team!

NTT DATA

Trusted Global Innovator